Human Capital Development – Resilient Cyber Physical Systems

Technical Report SERC-2017-TR-113

September 29, 2017

Principal Investigator:

Tom McDermott, Georgia Institute of Technology

Co-Principal Investigator:

Barry Horowitz, University of Virginia

Research Team:

Molly Nadolski, Georgia Institute of Technology
Paige Meierhofer, Georgia Institute of Technology
Nicola Bezzo, University of Virginia
Jack Davidson, University of Virginia
Ron Williams, University of Virginia

Contract Number: HQ0034-13-D-004
Report No. SERC-2017-TR-113
Task order 0075, RT 175

The Systems Engineering Research Center (SERC) is a federally funded University Affiliated Research Center managed by Stevens Institute of Technology.

This material is based upon work supported, in whole or in part, by the U.S. Department of Defense through the Office of the Assistant Secretary of Defense for Research and Engineering (ASD(R&E)) under Contract HQ0034-13-D-004 (Task Order 0075).

Table of Contents

List of Tables

List of Figures

This page intentionally left blank

Executive Summary

The research and education programs in computer and software security and resilience were advanced in the 1980's and 1990's with many formal approaches to system reliability, security, dependability, and safety – primarily in response to U.S Department of Defense needs. Since that time, the scale and complexity of critical computing systems has increased immensely, but without a related increased focus on research, knowledge, and education specifically addressing dependable and resilient computing. This significant need is critical for the software embedded systems that dominate defense missions, as well as emerging Internet of Things (IoT), distributed computing, and other commercial systems. A further area of concern is a lack of university investment in laboratory facilities that can simulate large scale cyber-physical systems (CPS). Most of the recent information security research and education programs focus on commercial information technology (IT) systems, and consequently, much of the recent university investment has focused on computer science and associates IT applications.

Formal research or studies in related curricula are also difficult to find. However, top universities such as Georgia Tech and the University of Virginia are now broadening their information security education programs to recognize specialized knowledge threads related to the unique demands of information systems, cyber-physical systems, and related policy concerns. In 2015 the National Academies Committee on 21st Century Cyber-Physical Systems Education explored requirements for education and training related to applications of the CPS domain. Their report, A 21st Century Cyber-Physical Systems Education, recommended "*the creation and evolution of undergraduate education courses, programs, and pathways so that engineering and computer science graduates have more opportunities to gain the knowledge and skills required to engineer cyber-physical systems*" [NAS, 2016]. Although this report focused on emerging commercial applications of CPS, the foundational knowledge applies equally to defense related systems.

This project conducted background research to develop a taxonomy that relates core characteristics of CPS, concepts of security and availability in CPS, and related core knowledge and skills associated with the development of such systems. A broad survey of existing education programs across more than 100 U.S. universities was conducted to characterize the existing undergraduate and graduate engineering and computer science education programs as related to emerging needs of CPS. These surveys were augmented by deeper dives into the education programs at our universities, including both curricula and laboratory programs, to develop a set of recommendations.

Based on the taxonomy development, we conclude in the DoD applications of resilient CPS there is a set of knowledge areas, skills, and competencies that can be derived from basic foundations and principles of dependability and security in computer and software systems, to particular aspects of dependability and security CPS, and finally to assurance principles that evaluate and verify their dependability and security. The unique aspects of military CPS can be viewed as an application area. We next looked at availability of education opportunities across the CPS domain.

After collection data on courses offered and labs/projects funded by these competitive engineering universities, it became clear that there is a lack of opportunities for students to learn more about CPS and computer security in general. For example, only four programs in our survey offered a degree with a dedicated CPS focus, and only two of these with a security component, highlighting the shortage of programs that can produce competent CPS engineers. Outside of the classroom, there was usually only one semi-thematically relevant project that students could participate in. These deficits illustrate the causes of the lack of qualified employees in CPS. Now that these results have been compiled, it is easier to provide evidence of an absence of attention to the critical topic that is security in these systems.

The combination of taxonomy development and survey results were used to produce a set of themes published curricula across U.S. university computer engineering and computer science programs to establish a set of themes that are indicators of the appropriate knowledge sets. These themes allowed us to combine knowledge of what constitutes a CPS with related curricula in computer engineering and computer science, and competencies associated with system assurance. This mapping will be useful in the development of future curriculum recommendations and competency models.

Very few academic institutions are currently supporting cybersecurity related laboratories that would support educational curriculum focused on resilience of cyber physical systems. However, advanced efforts in academia and industry related to cyber-attack resilience for physical systems are starting to emerge, including the use of laboratories to provide experimental results. These laboratory designs offer design opportunities for new laboratories that are focused on supporting educational needs. Resilience-focused solutions will demand future system designers who integrate solutions that are based upon technical and operational areas of knowledge that are not traditionally part of the cybersecurity curriculums that are now offered. In particular, techniques related to fault tolerant system design and understanding of attack taxonomies that integrate IT system attacks combined with control physical control system attacks are typically not part of a cybersecurity-related curriculum. Another outcome of the survey is the conclusion that model-based engineering techniques provide a significant opportunity for design and evaluation of potential resilience solutions.

The UVA team further investigated the concept of resilient CPS within a more specific taxonomy of threat attack methods and responses. They tested the resulting methods, processes and tools in an initial professional education setting with good results. Based upon these results it is recommended that the DoD consider establishing one or two new cyber physical system resilience education efforts that build upon the GaTech/UVA study outcomes and include the desire to continue to gather information about these efforts that will help to identify improvement opportunities based upon actual experience.

1 Introduction

This report provides the results of a 7-month research effort focused on developing information that could be used by the DoD in considering how to best employ existing academia-based resources regarding new education initiatives to accelerate the development of human capital to address resilience solutions related to cyber attacks on cyber physical systems. The effort was sponsored by the DoD through its University Affiliated Research Center (UARC), the multi-university Systems Engineering Research Center (SERC).

Recently, the DoD has undertaken a number of initiatives to better understand the vulnerability of their systems to a cyber-equipped adversary, and to address engineering processes that would help ensure DoD systems can complete their missions in the presence of such adversaries. There has been an intensive focus on securing computer networks and IT systems, and a great deal of investment in perimeter oriented defenses. Although this remains important, there is an increasing focus on the vulnerabilities of DoD weapon systems, and the general category of cyber-physical systems. Resilient Cyber-Physical Systems are systems that have been designed for operational resilience – the ability to anticipate, continue to operate correctly in the face of, recover from, and evolve to better adapt to advanced cyber threats [Mitre, 2015].

The DoD recognizes that the country's investment in education for cyber resilience has been mostly focused on IT systems. We are experiencing increasing numbers of attacks on control systems, attacks on critical infrastructure systems, and coordinated IT and control system attacks on everyday CPS such as automobiles and manufacturing equipment. There is a need to educate and train more engineers on the foundations, principles, and characteristics of security and resilience in CPS. The hypothesis of this research is that the U.S. educational system, which has responded to the critical need for security in IT systems, is lagging in the creation of professionals educated to deal with design for secure and resilient CPS.

1.1 OBJECTIVES

The DoD has focused investment for some time now on developing and sustaining a cyber-ready workforce. The objective of this research is to assess the ability and current state of U.S. university education to produce a workforce that can design, protect, and sustain secure and resilient CPS. This research is intended as an initial characterization of the educational landscape, and consists of the development of an appropriate taxonomy to describe a resilient CPS education, a survey of current university programs and resources in the domain, and a discussion of the challenges that may require further research.

This project was co-led by faculty from the Georgia Institute of Technology (GT) and the University of Virginia (UVA). GT conducted background research to develop a taxonomy that relates core characteristics of CPS, concepts of security and availability in CPS, and related core knowledge and skills associated with the development of such systems. GT also conducted a broad survey of existing education programs across more than 100 U.S. universities to characterize the existing undergraduate and graduate engineering and computer science education programs as related to emerging needs of CPS. These surveys were augmented by deeper dives into the education programs at our universities, including both curricula and laboratory programs, to develop a set of recommendations. UVA conducted a deeper exploration to develop an example Resilient CPS curriculum and laboratory experimentation program, and tested that in a professional education setting. The execution of these objectives will inform future research on the developing needs of the DoD workforce in the Resilient CPS domain.

1.2 SCOPE

This report explores the current state of academic curricula and educational programs in the U.S. focused on security and trust in CPS. In particular the research was conducted to address the needs for system security in the types of large scale CPS frequently developed in the defense domain, which can be characterized as unique physical platforms utilizing custom and off-the-shelf hardware and software components with connectivity to information and communications technologies. However in the process the general class of CPS and broader needs of dependable and secure systems were also addressed.

The research is intended to characterize the existing undergraduate, graduate, and professional engineering and computer science education programs in the U.S. as related to emerging needs of large scale cyber-physical systems. There are emerging needs of safety-critical, security-critical, and mission critical systems as they scale up in size and complexity, driven by mobility and information dependencies. Because of the emerging national focus on engineering needs in the CPS domain, the research focused on the general class of CPS systems and how they are being introduced into university education programs – it has not been limited to military systems. However the differences between military systems and a more general class of CPS are noted. In order to limit the scope of the survey at this point, the research only addresses U.S. university programs in Computer Science and Electrical and Computer Engineering. Education requirements in this domain are decidedly multi-disciplinary, and survey of coursework has been informed by computer science and software engineering as well as computer and system architectures, communication networks, formal modeling and simulation, verification strategies, and management and ethics. University investments to address these needs have also been addressed, as CPS often require expensive laboratory facilities that can accurate simulate large-scale control systems.

A Taxonomy of Resilient CPS: Part 1 of the project was led by GT and developed a taxonomy linking definitions of CPS and CPS resilience, related attributes for dependable and secure computing, competency models for hardware, software, and system security; and related bodies of knowledge and curricula guidance in computer science and electrical and computer engineering. This taxonomy was developed to inform the research and related surveys, it is not intended to be exhaustive and did not go through a process of community agreement.

A Survey of CPS Education Programs across U.S. Universities: Part 2 of the project was led by GT and conducted a survey of related undergraduate and graduate education programs in the fields of information security, computer science, computer engineering, and electrical engineering. The researchers surveyed degree programs and related curricula in U.S. universities that have content related to the taxonomy. The survey focused primarily on published course summaries. The research classified the survey data into a set of themes developed from the taxonomy.

Analysis of Resilient CPS Curriculum Approaches and Research Laboratory Requirements: Part 3 of the project was led by UVA and conducted a survey to help determine the current state and trends in academia related to the creation of laboratory capabilities for supporting cyber-physical system resilience education at the undergraduate and graduate levels, a survey of laboratory designs that support academic and industry research efforts that are experimental in nature and could potentially support class room education efforts, and application of those results to a resilient CPS education program provided by UVA in a professional development setting.

As part of the research, a set of future research challenges were identified for:

1. Developing a body of knowledge for resilient cyber-physical systems,
2. Developing a reference curriculum for SE of resilient cyber-physical systems and resilient computing systems, and
3. Addressing needs and opportunities for developing potential lab facilities related to resilient CPS.

2 Part 1: A Taxonomy of Resilient CPS

The first part of the project used background research and subject matter experts to define the set of concepts and a taxonomy that relates CPS, security, resilience, and associated core educational requirements. The taxonomy was used to create a set of topic areas for education programs relevant to the taxonomy.

2.1 BACKGROUND

The research and education programs in computer and software security and resilience were advanced in the 1980's and 1990's with many formal approaches to system reliability, security, dependability, and safety – primarily in response to U.S DoD needs. Since that time, the scale and complexity of critical computing systems has increased immensely, but without a related increased focus on research, knowledge, and education specifically addressing dependable and secure computing. This need is critical for the software embedded systems that dominate defense missions, as well as emerging IoT, distributed computing, and other commercial systems. The DoD is concerned that most university education in the U.S. is focused on IT systems, and that the education systems are not producing enough engineering graduates with knowledge and skills related to design of secure, safe, and dependable CPS, what we call resilient CPS. A further area of concern is a lack of university investment in laboratory facilities that can simulate large scale CPS. Because most of the growth in information security research and education programs focuses on commercial IT systems, much of the recent university investment has focused on large data centers and associated data analytics.

Formal research or studies in CPS and resilient computing related curricula are also difficult to find, although the domain is well researched. Since 2004, the Institute for Electrical and Electronics Engineers (IEEE) Technical Committee on Dependable Computing and Fault Tolerance has published through its magazine *Transactions on Dependable and Secure Computing*, articles related to "foundations, methodologies, and mechanisms that support the achievement–through design, modeling, and evaluation–of systems and networks that are dependable and secure to the desired degree without compromising performance." In the inaugural issue, Avižienis et al discuss definitions of dependability and security in CPS as a taxonomy of terms [Avižienis, 2004]. These publications, however, have not devoted any research to education needs. From 2006-2009, a European Union funded program titled Resilience for Survivability in Information System Technology (ReSIST) attempted to define a related graduate research curriculum; however, this effort has not been mentioned or targeted within U.S. educational communities [Simoncini, 2010] [ReSIST, 2008]. Until recently, there have been no large scale reference studies in U.S. universities systematically targeting the emerging needs of resilient CPS.

This is increasingly has become a recent concern and research priority, with groups such as the National Academy of Sciences (NAS) and National Institute of Standards and Technology (NIST) formally establishing research agendas and frameworks focused on CPS. Top universities such as Georgia Tech and the University of Virginia are now broadening their information security education programs to recognize specialized knowledge threads related to the unique demands of information systems, cyber-physical systems, and related policy concerns. In 2014 the European Union published their Next Generation Computing Research Priorities roadmap, shown in Figure 1, which illustrates the expanding influence of CPS in the computing domain and related dependability and security concerns.

In mid-2014, NIST established the CPS Public Working Group (CPS PWG) to bring together a broad range of CPS experts in an open public forum to help define and shape key characteristics of CPS, so as to better manage development and implementation within and across multiple "smart" application domains, including smart manufacturing, transportation, energy, and healthcare [NIST, 2016]. Through this framework, they seed to create a reference CPS description language on which tools, standards, and documented applications can be based, which will also allow more comprehensive analysis of CPS. In 2015, the National Academies Committee (within the

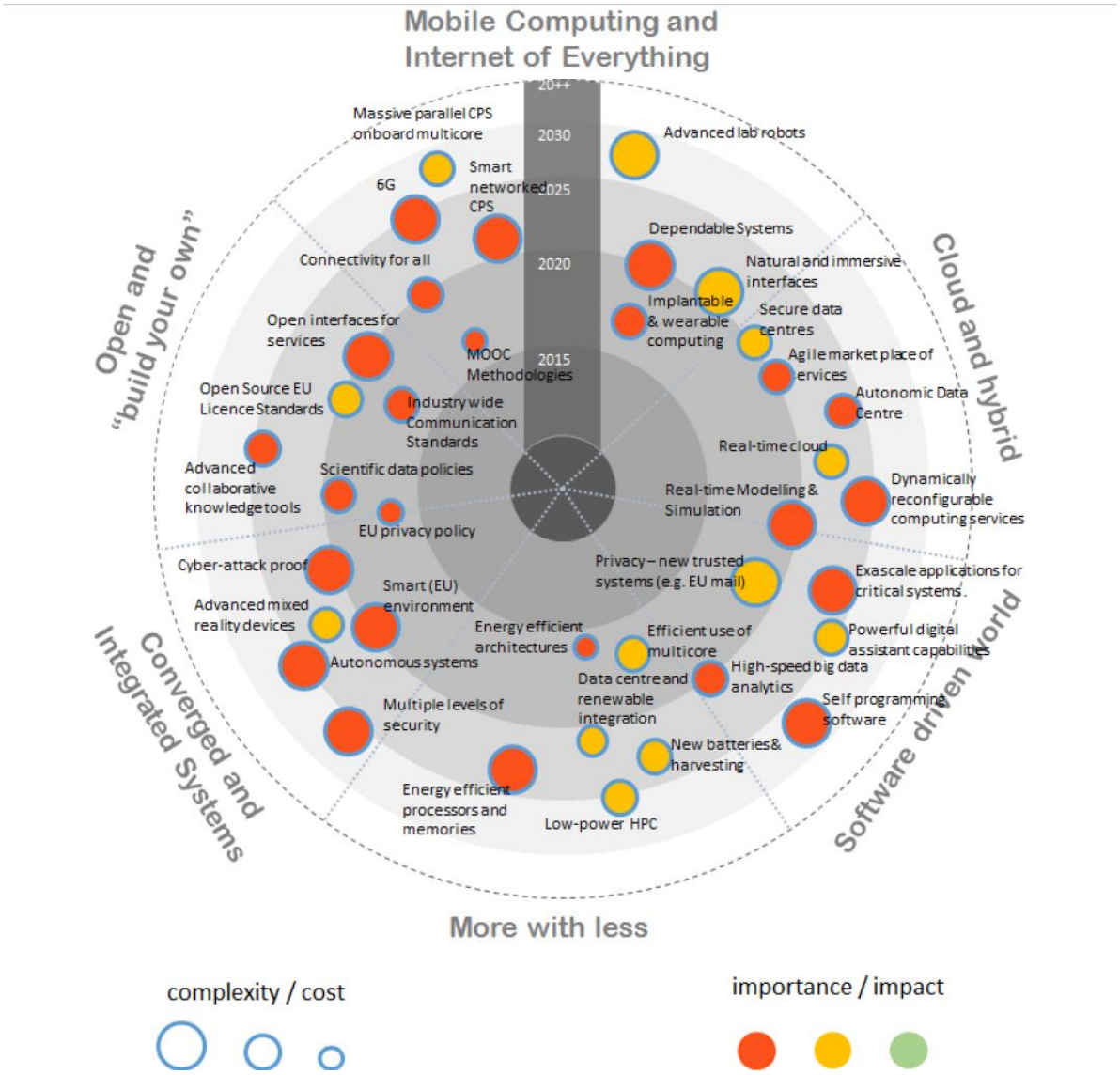

Figure 1. EU Next Generation Computing Research Priorities Roadmap [EU, 2014]

National Academies of Sciences) on 21st Century Cyber-Physical Systems Education explored requirements for education and training related to applications of the CPS domain. Their report, A 21st Century Cyber-Physical Systems Education, recommended "*the creation and evolution of undergraduate education courses, programs, and pathways so that engineering and computer science graduates have more opportunities to gain the knowledge and skills required to engineer cyber-physical systems*" [NAS, 2016]. Although this report focused on emerging commercial applications of CPS, the foundational knowledge applies equally to defense related systems. This project was conducted to characterize the existing undergraduate and graduate engineering and computer science education programs in the U.S. as related to emerging needs of large scale CPS. In particular, the research focused on the emerging needs of safety-critical, security-critical, and mission critical systems as they scale up in size and complexity, driven by mobility and information dependencies. Critical knowledge requirements in this domain are driven by fundamental systems engineering trades that balance formal verification versus cost. Education requirements are decidedly multi-disciplinary, extending well beyond computer science and software engineering into computer and system architectures, communication networks, formal modeling and simulation, verification strategies, and management and ethics. University investments to address these needs often require expensive laboratory facilities that can accurate simulate large-scale control systems.

With this background, our research started with development of a taxonomy of related attributes for dependable and secure computing, followed by a broad survey of related undergraduate and graduate education programs in the fields of information security, computer science, computer engineering, and electrical engineering, then augmented with deeper studies of specific curricula and research facilities necessary to produce the desired knowledge, skills, and competencies. In order to adequately define the context, the next section presents a taxonomy that relates DoD concepts of mission assurance to the characteristics and applications of CPS, then more specifically to principles and attributes of hardware and software assurance in these systems, and finally to related bodies of knowledge and standard curriculum recommendations.

2.2 A TAXONOMY TO RELATE "RESILIENT CPS" TO EDUCATION IN ENGINEERING AND COMPUTING DOMAINS

2.2.1 WHAT IS A CPS?

According to the National Science Foundation, CPS are "engineered systems that are built from, and depend upon, the seamless integration of computational algorithms and physical components" [NSF, 2016]. According to Berkeley's Electrical Engineering and Computer Science program's CPS overview website, CPS are characterized by their relationship between computers and networks which control physical processes, using feedback loops that affect computations and vice versa [UC Regents, 2017]. These highly interconnected and integrated systems provide new functionalities to improve quality of life and enable technological advances in critical areas, such as personalized health care, emergency response, traffic flow management, smart manufacturing, defense and homeland security, and energy supply and use. In addition to CPS, there are many words and phrases (Industrial Internet, Internet of Things (IoT), machine-to-machine (M2M), smart cities, and others) that describe similar or related systems and concepts [NIST]. There is significant overlap between CPS and IoT concepts, wherein CPS and IoT are sometimes used interchangeably; as such, the approach described in the NIST CPS Framework can be considered to be equally applicable to IoT [NIST]. The technology builds on the older (but still very young) discipline of embedded systems, computers and software embedded in devices whose principal mission is not computation, such as cars, toys, medical devices, and scientific instruments. Their distinction from embedded systems is important. Embedded systems are more focused on the computing characteristic, whereas CPS highlight the conjunction with the physical dynamics alongside the dynamics of software and networks.

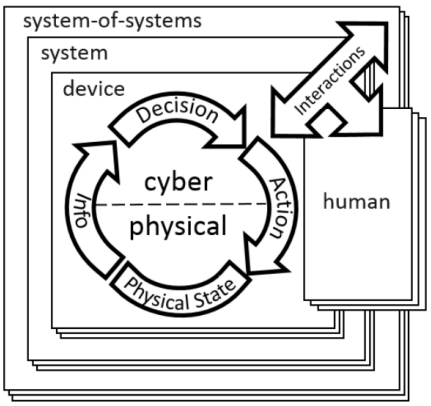

Figure 2. CPS Conceptual Model (Source: NIST, 2016)

The impacts of CPS will be pervasive and substantial, and we are already seeing evidence of its potential vis-à-vis autonomous vehicles, intelligent buildings, smart energy systems, robots, and smart medical devices. Figure 3 provides an idea of the breadth of CPS applications, many of which will impact military missions over time. While they bring promise of innovation, they also bring many risks, including system safety, privacy, and unintended effects of machine failure. The risks we focus on from here include dependability and security. Two of the challenges faced by CPS include ensuring dependability and security as the systems scale up and ensuring security in both the computer and physical systems. Unfortunately, due to a lack of resilient system solutions, there currently exists a gap between efficiency and security.

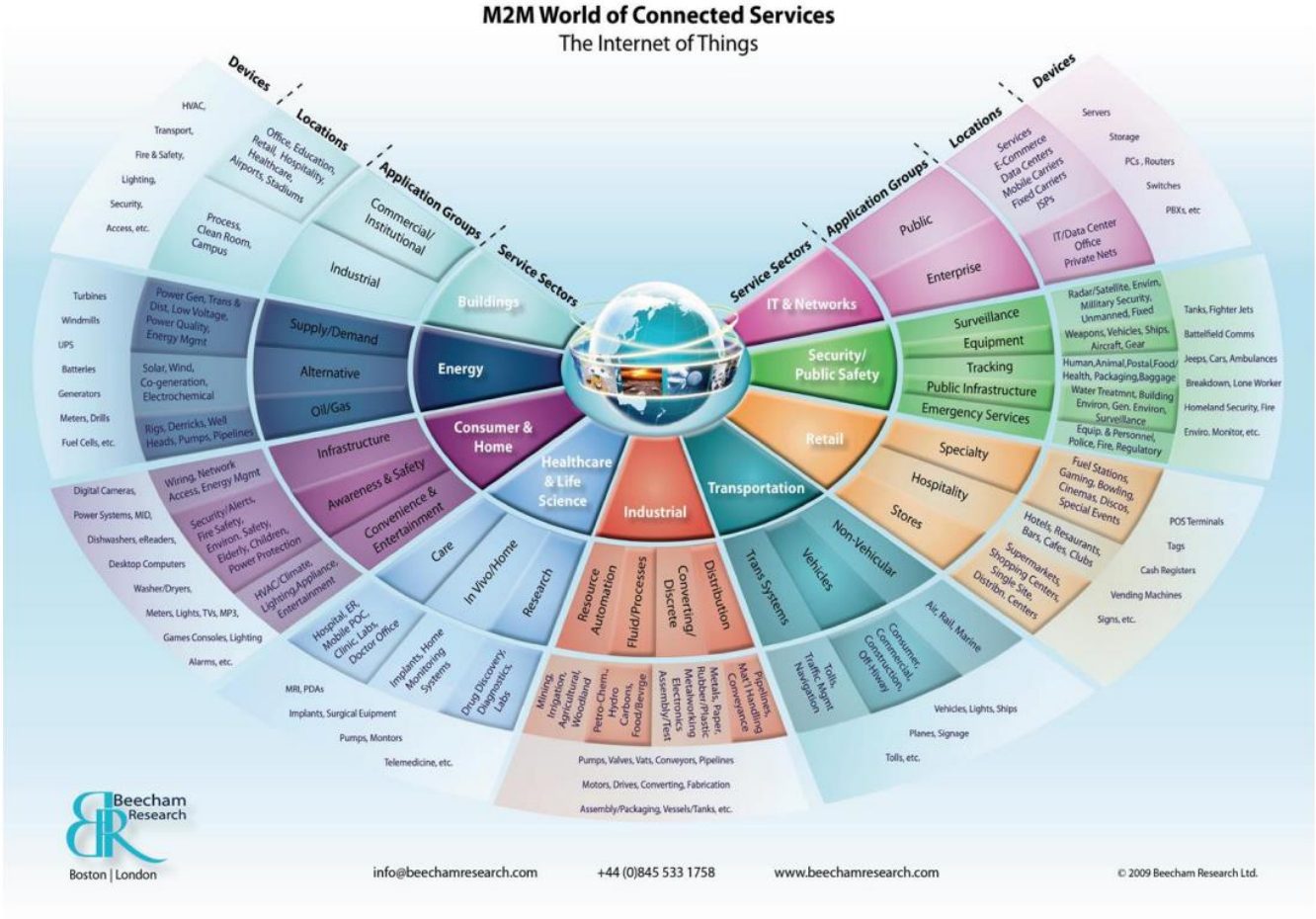

Figure 3. Segmentation of M2M Market

2.2.2 WHAT CONSTITUTES RESILIENCE IN CPS?

One of the more pressing challenges in providing cybersecurity for CPS is resiliency capability needs. Traditional approaches to cybersecurity, privacy, reliability, resilience, and safety may not be sufficient to address the risks to CPS. The nature of CPS increases the possibilities of breach and presents different types of vulnerabilities. CPS have exposed physical world interfaces that may be vulnerable to new types of intrusions. CPS are frequently systems of systems (SoS), increasing attack surfaces, system diversity and complexity, and difficulty in identifying system boundaries. Therefore, the architectural constructs should be able to be applied recursively or iteratively to support this nested nature of CPS and sensing/control and computational nature of CPS generally leads to emergent higher levels of behavior and system intelligence [NIST, 2016]. The NIST report identifies the following aspects that shape resilience in understanding the multi-disciplinary nature of these issues, which clearly require human, control, and cyber systems to address holistically, listed in table 1.

	Aspects That Shape CPS Resilience
Unexpected condition adaptation	• Achievable hierarchy with semi-autonomous echelons: The ability to have large scale, integrated supervisory control methodologies that implement graceful degradation.
	• Complex interdependencies and latency: Widely distributed, dynamic control system elements organized to prevent destabilization of the controlled system.
Human interaction challenges	• Human performance prediction: Humans possess great capability based upon knowledge and skill, but are not always operating at the same performance level.
	• Cyber awareness and intelligent adversary: The ability to recognize and mitigate cyber-attacks is necessary to ensure the integrity of the control system.
Goal conflicts	• Potentially conflicting goals and flawed understanding of the factors affecting system behavior: Besides stability, security, efficiency and other factors influence the overall criteria for performance of the control system.
	• Lack of state awareness: Raw data must be translated to information on the condition of the process and the control system components.

Table 1. Aspects That Shape CPS Resilience (NIST, 2016)

General concepts of CPS resilience are founded in engineering concepts of dependable and secure systems. The IEEE Committee on Dependable Computing and Fault Tolerance relates dependability and security in general as the ability to avoid service failures, and list interrelated foundational attributes of availability, reliability, safety, integrity, confidentiality, and maintainability. These attributes work together to ensure the system's successful application. *Dependability* is specifically characterized in a CPS by the unique factor of inter-system dependence. The dependence of the cyber system on the physical system thus represents the extent to which the cyber system's dependability is (or would be) affected by that of the physical system. Security is a "composite of the attributes of confidentiality, integrity, and availability, requiring the concurrent existence of 1) availability for authorized actions only, 2) confidentiality, and 3) integrity with 'improper' meaning 'unauthorized.'" [Avižienis, 2004].

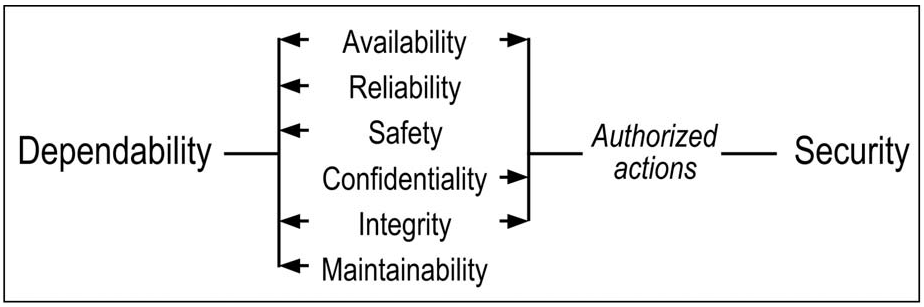

Figure 4. Dependability and Security Attributes (Avižienis, 2004).

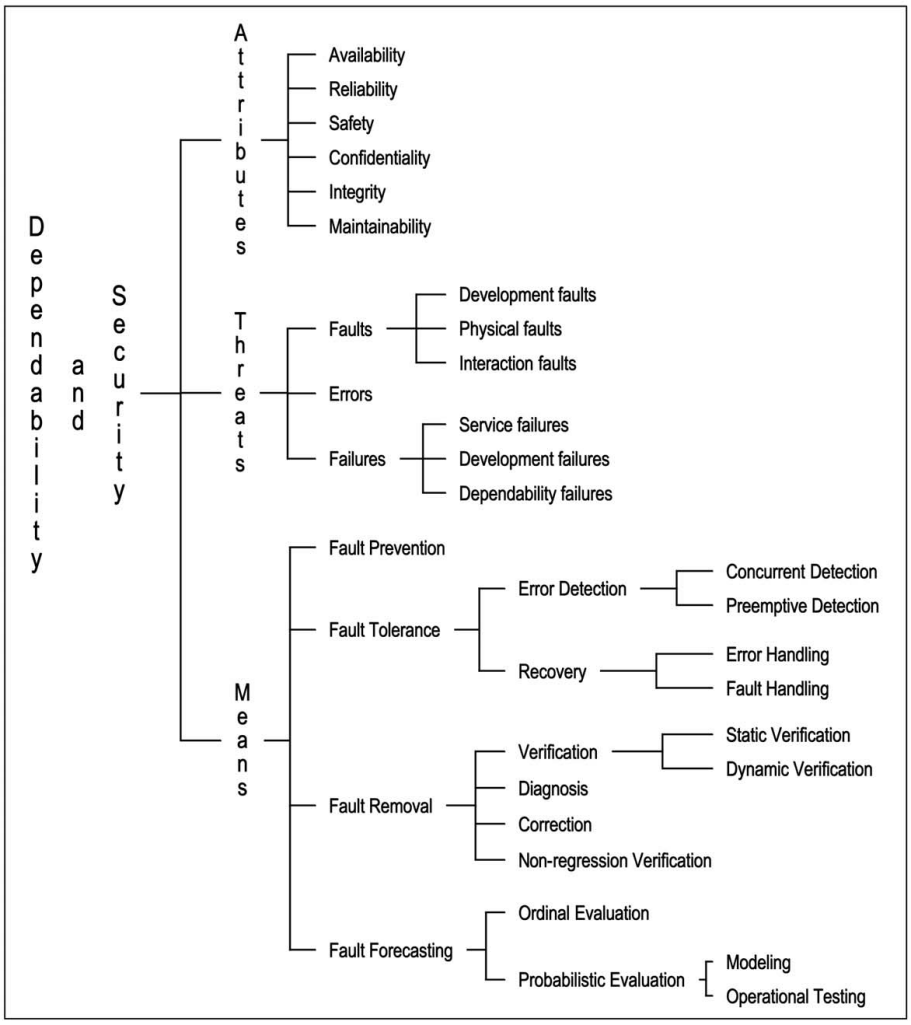

Figure 5. The Dependability and Security Tree (Avižienis, 2004)

The full taxonomy is depicted in a dependability and security tree, shown in Figure 5. This taxonomy is reflective of the engineering considerations of CPS resilience in terms of system service failures, which would be reflected in a resilience framework as continuity of system service. The taxonomy recognizes an alternate definition of dependability as the ability of a system to avoid service failures that are more frequent or more severe than is acceptable. This definition is closer to concepts of resilience. The taxonomy also introduces the relationship between dependability and trust as "The dependence of system A on system B represents the extent to which System A's dependability is (or would be) affected by that of System B. Trust is accepted dependence." [Avižienis, 2004].

The cyber adversary represents a multi-level threat to CPS. What has changed significantly since 2004 is the nature of the cyber threat. Within a CPS, cyber security meets physical security, and this is the emerging CPS challenge. Even if the cyber domain is completely secure and the physical domain is completely secure, the system still may not be secure because of the domains' interactions and dependence on one another. Research into the domains' interdependence is severely lacking and in need of model and definition development, and education needs are just as pressing. A deeper discussion of cyber adversary related faults are discussed in part 3.

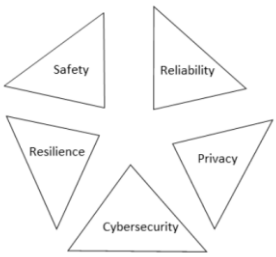

Figure 6. Evolution of Systems Design Property Silos (NIST, 2016)

NIST highlights the concern of resilience in terms of trustworthiness, related to the ability of the CPS to withstand instability, unexpected conditions, and gracefully return to predictable, but possibly degraded, performance. However, given the multi-level threats and 'cross-cutting' potential given all of the activities of the components of CPS, there will be trade-offs between the concerns. Corrective action taken to bolster its safety may then reduce the effectiveness of the actions for cyber-security, resilience or reliability [NIST, 2016]. The unique qualities of CPS must be considered when designing and developing secure CPS. Furthermore, trustworthy CPS architectures must be based on a detailed understanding of the physical properties and constraints of the system, design activities should be based on threats to resilience, cyber-physical interdependencies, cognitive human based aspects, and cyber-physical cognitive aspects. Analysis in support of design activities must include creation and simulation of up-to-date adversary models [NIST, 2016].

The properties of safety, reliability, privacy, cybersecurity, and resilience have, for the most part, evolved within distinct silos (see Figure 6). Historically, systems design has occurred within disparate disciplines. Large systems engineering and integration projects often have property-specific leads, who represent discrete viewpoints within the trade-off process overseen by the chief systems engineer/integrator. Functional requirements often have caused engineers and designers to prioritize each property differently, based on domain-specific (energy, manufacturing, transportation, etc.) requirements and perspectives, but achieving a certain level of success in each property typically is vital to the overall success of the system. Industry trends suggest that discrete systems engineering disciplines are converging toward increased interdependency as illustrated in Figure 7. This is particularly important for CPS, in which systems-based holistic thinking will be critical to supporting objectives such as safety, reliability, resilience, privacy, and security. The relative importance and interaction of the various risk-related properties must be considered so that problems arising with respect to one property, or protections inserted to address one dimension of concern, do not compromise other primary system objectives or cause deleterious unintended effects. An interdisciplinary approach to systems design and integration is, therefore, required to establish an overall SoS design objective and support appropriate trade-offs in the service of that objective, if possible.

Figure 7. Recommended Interdisciplinary Design Approach to CPS Engineering (NIST, 2016)

2.2.3 WHAT CONSTITUTES CPS RESILIENCE IN DOD SYSTEMS?

Because of the unique characteristics of military systems, it is important to analyze the DoD context as a specialization area in CPS education. Whereas the general definitions of threats to dependability and security are focused on disruption of operational services, the DoD expands these definitions to effects on operational missions. Are there unique educational foundations that will be necessary to address the DoD focus on military operational missions?

The DoD defines the operational resilience of CPS in a number of ways. DoD Instruction (DoDI) 8500.01 on Cybersecurity recommends that hardware and software components of systems "have the ability to reconfigure, optimize, self-defend, and recover with little or no human intervention." DoDI 8500.01 further defines three conditions for operational resilience: the systems are trustworthy, missions of these systems can tolerate degradation or loss of resources, and the systems have designs that provide means to prevail in the presence of adverse events [DoDI 8500.01, 2014]. These conditions reflect common resilient CPS principles, but the context is somewhat different from commercial CPS.

Within the context of military cyber operations and threats, CPS resilience can be interpreted as the ability of a system to maintain its operational mission effectiveness while under adversary offensive cyber operations, and to manage the risk of adversary exploitation of the system for intelligence purposes [Holtzman, 2017]. Figure 9 depicts the unique issues associated with DoD systems. Military weapon systems differ from commercial CPS in that they are tailored to specific missions, lack standardization, and use much more customized hardware and software. They also have different threats with different intent than commercial CPS. Although the foundations and principles of CPS resilience remain the same for both types of systems, the DoD has some unique application areas. With respect to educational needs, we conclude that basic foundations and principles of secure CPS are the same in all application domains, while the need for practical experience will be specific to the domain. This suggests that universities must invest in domain driven laboratory facilities that cover a range of CPS applications, some of which are germane to military systems or similar.

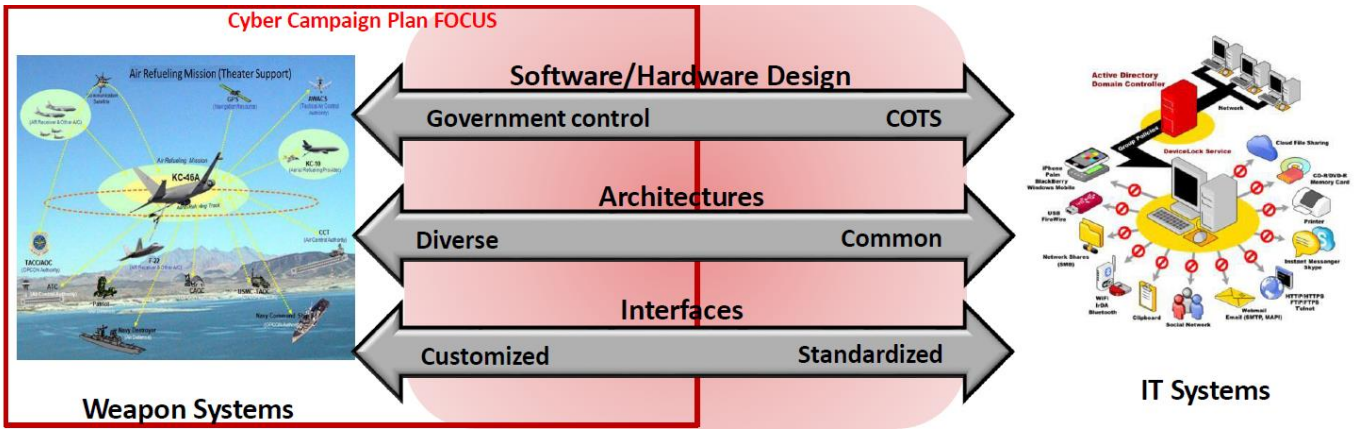

Figure 8. DoD Weapon System CPS Resiliency Focus (Holtzman, 2017)

In deriving a taxonomy of CPS security with respect to educational needs, we need to ensure the military application domains are represented. We follow basic taxonomies of CPS with DoD knowledge areas. The DoD lists five knowledge areas related to resilient CPS: the threat, the mission, system vulnerabilities, approaches for resilient design, and validation of the system. Desirable principles of resilient CPS include [Reed]:

1. Concepts of secure access control to and use of the system and system resources
2. Understanding of design concepts that minimize exposure of vulnerabilities to external threats (techniques such as design choice, component choice, security techniques, system update management, etc.)
3. Understanding of design patterns that protect and preserve system functions or resources (segmentation, separation, isolation, partitioning, etc.)
4. Approaches to monitor, detect and respond to security anomalies
5. Approaches to maintain system availability under adverse conditions
6. Understanding of network operations and external security services."

Again, we conclude that none of these principles are unique to military CPS, other than the context of secure access control in military systems that contain classified information.

All of the taxonomy at this point reflects a multi-disciplinary knowledge basis that includes both engineering and computer science disciplines, as well as knowledge of the operational characteristics of CPS in the operational or mission context that is specific to the application. All of the background research so far aligns well with a notional taxonomy was presented by Reed as reflected in Figure 10. In this figure the yellow highlighted items are the characteristics of the CPS, the grey highlights represent the CPS principles, the blue are the engineering processes

to assure resilient CPS, and the orange highlights are the types of systems of interest to the DoD. This taxonomy highlights "maximum reasonable assurance" as a description of trust in military CPS. This is not a divergence of concepts in the taxonomy, but it does imply a set of methods and processes for "assured services and missions" that are different in the DoD domain. Competencies in the assurance domain are an important part of education in the DoD, and justify a further emphasis in this study.

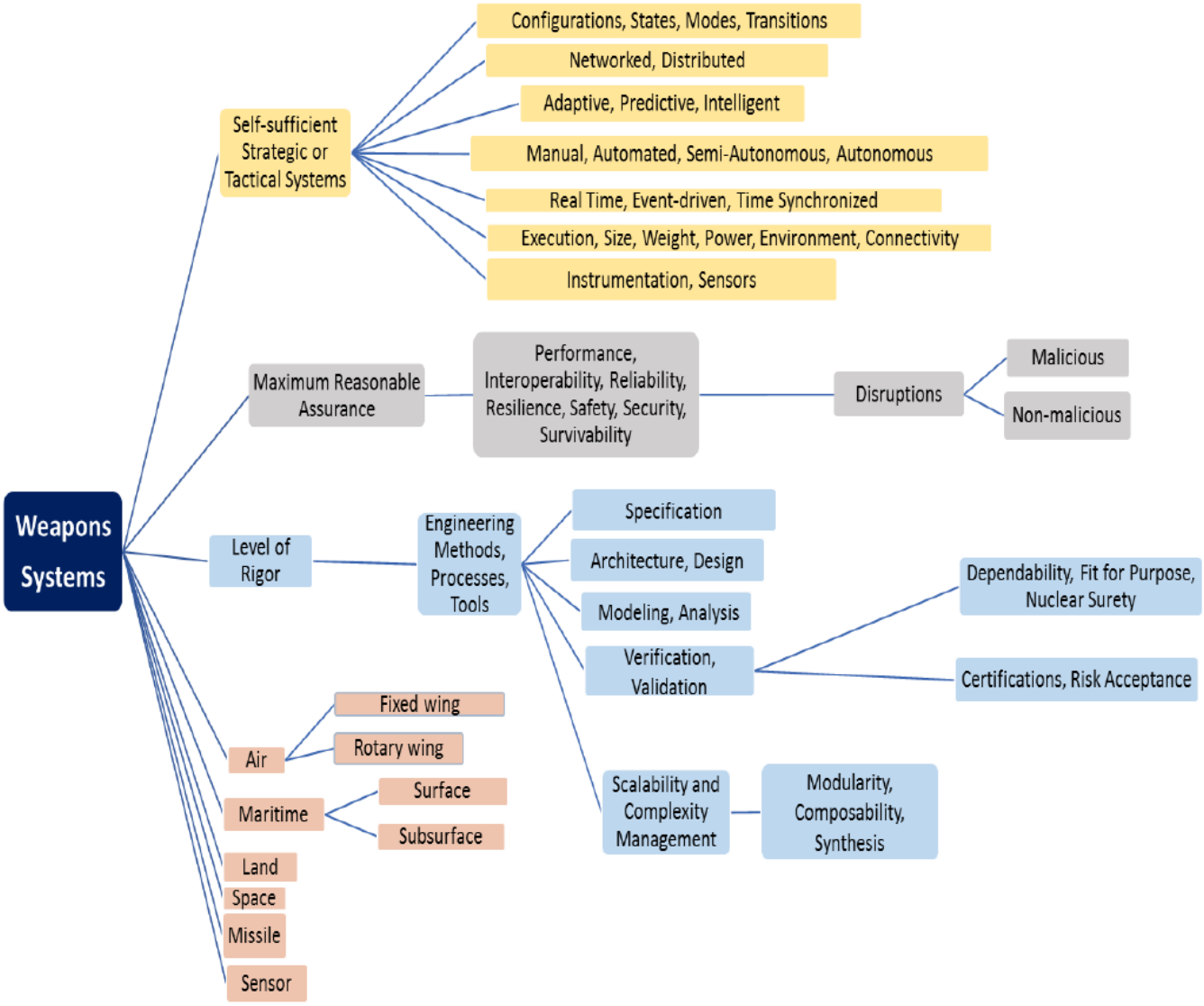

Figure 9. Engineering Considerations for Cyber-Resilient Weapon Systems [Reed, 2016].

The Software Assurance Competency model [CMU/SEI-2013-TN-004, 2010] described by the Software Engineering Institute (SEI), defines "maximum reasonable assurance" in terms of software assurance as:

> *"Application of technologies and processes to achieve a required level of confidence that software systems and services function in the intended manner, are free from accidental or intentional vulnerabilities, provide security capabilities appropriate to the threat environment, and recover from intrusions and failures."*

This is extended to a systems level, or a CPS, by adding to software assurance the need for hardware and secure architecture principles. Based on a discussion with the International Council on Systems Engineering's (INCOSE)

System Security Working Group, they are contemplating three competency areas relevant to resilient CPS [INCOSE, 2015]:

- Trusted Supply Chain Management – trust in acquired components of the system,
- Secure Architecture Design – a system architecture and requirements that produce a secure solution,
- Software Assurance Assessment – based on the SEI competency model.

Thus we conclude in the DoD applications of resilient CPS there is a set of knowledge areas, skills, and competencies that can be derived from basic foundations and principles of dependability and security in computer and software systems, to particular aspects of dependability and security CPS, and finally to assurance principles that evaluate and verify their dependability and security. The next sections integrate several related competency and educational curriculum studies together to begin the derivation of a set of skills and competencies necessary to the design of resilient CPS.

2.2.4 WHAT ARE THE SKILLS AND COMPETENCIES NEEDED TO DEVELOP RESILIENT CPS?

In this section we relate the taxonomy of resilient CPS to a further taxonomy that describes the knowledge areas, skills, and competencies of a "CPS engineer." The NAS report uses the terms "CPS engineering" and "CPS engineer" to classify people and their skills and knowledge necessary for design in the CPS domain. CPS engineering as a domain targets the interrelated characteristics of physical aspects and cyber aspects of a system. It is an application area requiring a set of foundational skills related to computing in both the physical and cyber worlds; multi-disciplinary knowledge of CPS principles that bridge elements of the physical sciences, computer engineering, and computer science; and practical knowledge of the attributes and characteristics of different types of CPS systems, including concepts of dependability and security in CPS [NAS, 2016].

The NAS report lists the need for knowledge of the principles used in CPS, foundational knowledge in six key areas of CPS, and knowledge of system characteristics and attributes of CPS in their operational environment. The report recommends development of CPS-focused courses within engineering education programs as well as CPS applications that build experience in the domain. Table 2 outlines the recommendations for this educational program.

Table 2. NAS CPS Educational Program Recommendations

CPS principles	CPS foundations to cover	CPS characteristics to cover
Communication and Networking	Basic computing concepts, including software engineering	Security and privacy
Real time systems	Physical world computing, including sensors, actuators, and real-time control	Interoperability
Embedded systems, both hardware and software	Discrete and continuous mathematics	Discrete and continuous mathematics
Physical world computing, including safety, reliability, security, performance, and risk management	Cross-cutting application of sensing, actuation, control, communication, and computing	Reliability and dependability
Human interaction with CPS, including ease of use	Modeling of heterogeneous and dynamic systems integrating control, computing, and communication	Power and energy management
	CPS system development (emphasizing concepts of resilience and safety, test and verification)	Safety
		Stability and performance
		Human factors and usability

According to the report, “These considerations are often essential in ensuring a system will operate with increased confidence in the presence of uncertainty and with acceptable levels of risk” [NAS, 2016]. A key aspect of education in this domain is to develop working knowledge of the methods and tools to ensure these characteristics are met, what we call system assurance. This is a key focus of DoD applications. Although no CPS assurance competency model exists, we can start with the existing software assurance competency models and extend them to system level applications using the goals of the INCOSE competency model development or another effort.

According to the SEI Software Assurance Competency model [CMU/SEI-2013-TN-004, 2010], the needed competencies have a base in already existing computer engineering skills, but dive deeper into security and physical systems. This model was developed in order to help evaluate professionals and potential employees on their software assurance skills, as well as to provide guidance to academic or training organizations that develop security courses. It is also useful in recommending curricula guidance by providing information about industry needs and expectations for competent software assurance professionals. These competencies help to provide direction and a progression for the development and career planning of software assurance professionals. The following competencies in Table 3 outline the entry level requirements for a career dealing with CPS.

Table 3. Entry Level Competencies for a Career Dealing with Assurance [CMU/SEI-2013-TN-004, 2010]

Competency	Description
System/software lifecycle processes	Able to manage the application of a defined lifecycle software process for a small project
Software Assurance Processes	Able to apply methods, processes, and tools to asses assurance
Risk Management Concepts	Understanding of risk analysis and risk management, including threat modeling
Risk Management Processes	Able to identify and describe risks in a project; able to analyze likelihood and severity; understanding of risks; understanding of risks in the acquisition of contracted software; employment of mitigation tasks
Assurance Assessment Concepts	Basic understanding of assurance assessment methods
Measurement for Assessing Assurance	Able to apply tools and documentation support for assessment processes
Business Case for Assurance	Able to apply a business case tradeoff analysis and determine validity of the case
Managing Assurance	Understanding the importance of system assurance in the lifecycle
Compliance Considerations	Understand the importance of and able to apply compliance considerations, laws, and policies
System Security Assurance	Understanding of safety and security risks in critical systems; understanding of the variety of methods attackers use to damage systems; understanding of known attacks and how security practices are used against them; understanding the legal and ethical considerations in attacks versus assurance capabilities
System Functionality Assurance	Awareness of and ability to apply current technology used for functionality assurance; understand the importance of and ability to engage in the tasks associated with system functional assurance; ability to apply methods and tools for structured and functional analysis
System Operational Assurance	Understand and support creation of security policies and procedures
Other	Understand and support installation and configuration of security monitors and controls; understanding and implementation of effective responses to operational system events

Given that most entry-level engineering and computer science positions are filled by Bachelor’s degree holders, it is important to incorporate resilient CPS education into the undergraduate engineering and computer science

curricula. In the educational domain, the NAS report outlines the foundations needed to build a successful workforce. The competencies outlined above with the creation of a workforce skilled in engineering CPS will allow the deployment of increasingly capable, adaptable, and trustworthy systems. Engineers responsible for developing CPS but lacking the appropriate education or training may not fully understand at an appropriate depth, on the one hand, the technical issues associated with the CPS software and hardware or, on the other hand, techniques for physical system modeling, energy and power, actuation, signal processing, and control. In addition, these engineers may be designing and implementing critical systems without appropriate formal training in CPS methods needed for verification and to assure safety, reliability, and security. A workforce with the appropriate education, training, and skills will be better positioned to create and manage the next generation of CPS solutions. Building this workforce requires attention to educating the future workforce with all the required skills as well as providing the existing workforce with the needed supplementary education.

2.2.5 WHAT SHOULD A CURRICULUM IN RESILIENT CPS INCLUDE?

Undergraduate and Graduate curricula for CPS specialization live at the intersection between computer engineering and computer science bodies of knowledge. The Association of Computing Machinery (ACM) provides reference curricula for both subject areas [ACM1, 2013 & ACM2, 2015]. These reports in general cover all of the knowledge areas that would be associated with CPS. What is needed is an appropriate curriculum thread or specialized degree that combined these curricula around applications of CPS. According to the NAS recommendations this should include a dedicated first year course or set of courses providing an introduction to CPS and a third year practical laboratory experience in one or more CPS platforms [NAS, 2016]. The curriculum would then include a set of foundational and principles-driven courses drawn from electrical and computer engineering and computer science domains, with practical experience in CPS applications and characteristics.

The ACM draft Computer Engineering Curriculum guidelines, published for comment in 2016, lists 13 knowledge areas (KAs) and bodies of knowledge in the domain. The latest ACM Computer Science Curriculum Guidelines, published in 2014, identify 16 KAs and bodies of knowledge. In tables 4 and 5 we list only the bodies of knowledge that the previous taxonomy development list as applicable to secure CPS. The other foundations in this domain are not listed but the curriculum assumes they are covered.

In Part 2 of this report we assess the competency and curriculum guidance against a survey of the courses actually being taught across U.S. University engineering and computer science programs. The combination of the taxonomy assessment, competency models, and curriculum guidance allowed us to develop a set of themes that relate existing university programs to the educational needs of resilient CPS.

Table 4. Computer Engineering Knowledge Areas and Bodies of Knowledge (ACM1, 2013)

Knowledge Areas	Resilient CPS Selected Bodies of Knowledge
CE-CAE Circuits and Electronics	
CE-CAL Computing Algorithms	
CE-CAO Computer Architecture and Organization	Instruction set architecture; Measuring performance; Computer arithmetic; Processor organization; Memory system organization and architectures; Input/Output interfacing and communication; Peripheral subsystems; Multi/Many-core architectures; Distributed system architectures
CE-DIG Digital Design	
CE-ESY Embedded Systems	Characteristics of embedded systems; Basic software techniques for embedded applications; Parallel input and output; Asynchronous and synchronous serial communication; Periodic interrupts, waveform generation, time measurement; Data acquisition, control, sensors, actuators; Implementation strategies for complex embedded systems; Techniques for low-power operation; Mobile and networked embedded systems; Advanced input/output topics; Computing platforms for embedded systems
CE-NWK Computer Networks	Network architecture; Local and wide area networks; Wireless and mobile networks; Network protocols; Network applications; Network management; Data communications; Performance evaluation; Wireless sensor networks
CE-PFP Professional Practice	
CE-SEC Information Security	Data security and integrity; Vulnerabilities and exploitation; Resource protection models; Secret and public key cryptography; Message authentication codes; Network and web security Authentication; Trusted computing; Side-channel attacks
CE-SET Strategies for Emerging Technologies	
CE-SGP Signal Processing	
CE-SPE Systems and Project Engineering	Project management principles; Human-computer interaction; Risk, dependability, safety and fault tolerance; Hardware and software processes; Requirements analysis and elicitation; System specifications; System architectural design and evaluation; Concurrent hardware and software design; System integration, testing and validation; Maintainability, sustainability, manufacturability
CE-SRM Systems Resource Management	Managing system resources; Real-time operating system design; Operating systems for mobile devices; Support for concurrent processing; System performance evaluation; Support for virtualization
CE-SWD Software Design	Programming constructs and paradigms; Problem-solving strategies; Data structures; Recursion; Object-oriented design; Software testing and quality; Data modeling; Database systems; Event-driven and concurrent programming; Using application programming interfaces; Data mining; Data visualization

Table 5. Computer Science Knowledge Areas and Bodies of Knowledge (ACM2, 2015)

Knowledge Areas	Resilient CPS Selected Bodies of Knowledge
AL - Algorithms and Complexity	Analysis; Algorithmic Strategies; Data Structures and Algorithms; Automata, Computability, and Complexity
AR - Architecture and Organization	Digital Logic and Digital Systems; Machine Level Data Representation; Memory System Architecture; Interfaces and Communication
CN - Computational Science	Introduction to Modeling and Simulation
DS - Discrete Structures	Sets, Relations, and Functions; Basic Logic; Proof Techniques; Basics of Counting; Graphs and Trees; Discrete Probability
GV - Graphics and Visualization	Fundamental Concepts
HCI - Human-Computer Interaction	HCI Foundations; Designing Interaction
IAS - Information Assurance and Security	Foundational Concepts; Principles of Secure Design; Defensive Programming; Threats and Attacks; Network Security; Cryptography; Web Security; Platform Security; Security Policy & Governance; Secure Software Engineering
IM - Information Management	IM Concepts; Database Designs; Data Modeling
IS - Intelligent Systems	IS Fundamentals; Basic Search Strategies; Knowledge Representation and Reasoning; Basic Machine Learning Electives: Agents; Robotics
NC - Networking and Communications	NC Introduction; Networked Applications; Reliable Data Delivery; Routing and Forwarding; Local Area Networks; Resource Allocation; Mobility; Social Networking
OS - Operating Systems	Introduction; OS Principles; Concurrency; Scheduling and Dispatch; Memory Management; Security and Protection Electives: Device Management; Real-time and Embedded Systems; Fault Tolerance
PBD - Platform-based Development	Mobile Platforms and Industrial Platforms are electives; Other CPS areas like transportation, etc. might be relevant
PD - Parallel and Distributed Computing	Parallelism Fundamentals; Parallel Decomposition; Communication and Coordination; Parallel architecture; distributed systems; Cloud Computing; Formal Models and Semantics
PL - Programming Languages	Object Oriented Programming; Functional Programming; Event-Driven and Reactive Programming; Basic Type Systems; Program Representation; Language Translation and Execution
SDF - Software Development Fundamentals	Algorithms and Design; Fundamental Programming Concepts; Fundamental Data Structures; Development Methods
SE - Software Engineering	Processes; Project Management; Tools and Environments; Requirements Engineering; Software Design and Construction; Verification and Validation; Evolution; Reliability; Formal Methods
SF - Systems Fundamentals	Computational Paradigms; Cross-Layer Communications; States and State Machines; Parallelism; Evaluation; Resource Allocation and Scheduling; Proximity; Virtualization; Reliability; Quantitative Evaluation
SP - Social Issues and Professional Practice	Social Context; Analytical Tools; Professional Ethics; Intellectual Property; Privacy; Professional Communication; Sustainability; History; Economies of Computing; Security Policies, Laws, and Crime

3 Part 2: A Survey of CPS Education Programs across U.S. Universities

In order to survey the state of CPS education, the research looked into published curricula across U.S. university computer engineering and computer science programs to establish a set of themes that are indicators of the appropriate knowledge sets. These themes were used to classify survey data and are not intended to represent any official curriculum recommendations, although the themes were linked to specific bodies of knowledge in the related ACM guidance. The undergraduate themes are shown in figure 10.

Additional themes related to graduate level education include Secure Coding and Programming Languages; Embedded Systems; Sensors and Power Networks; Dependability, Risk, & Reliability; and Wireless Security.

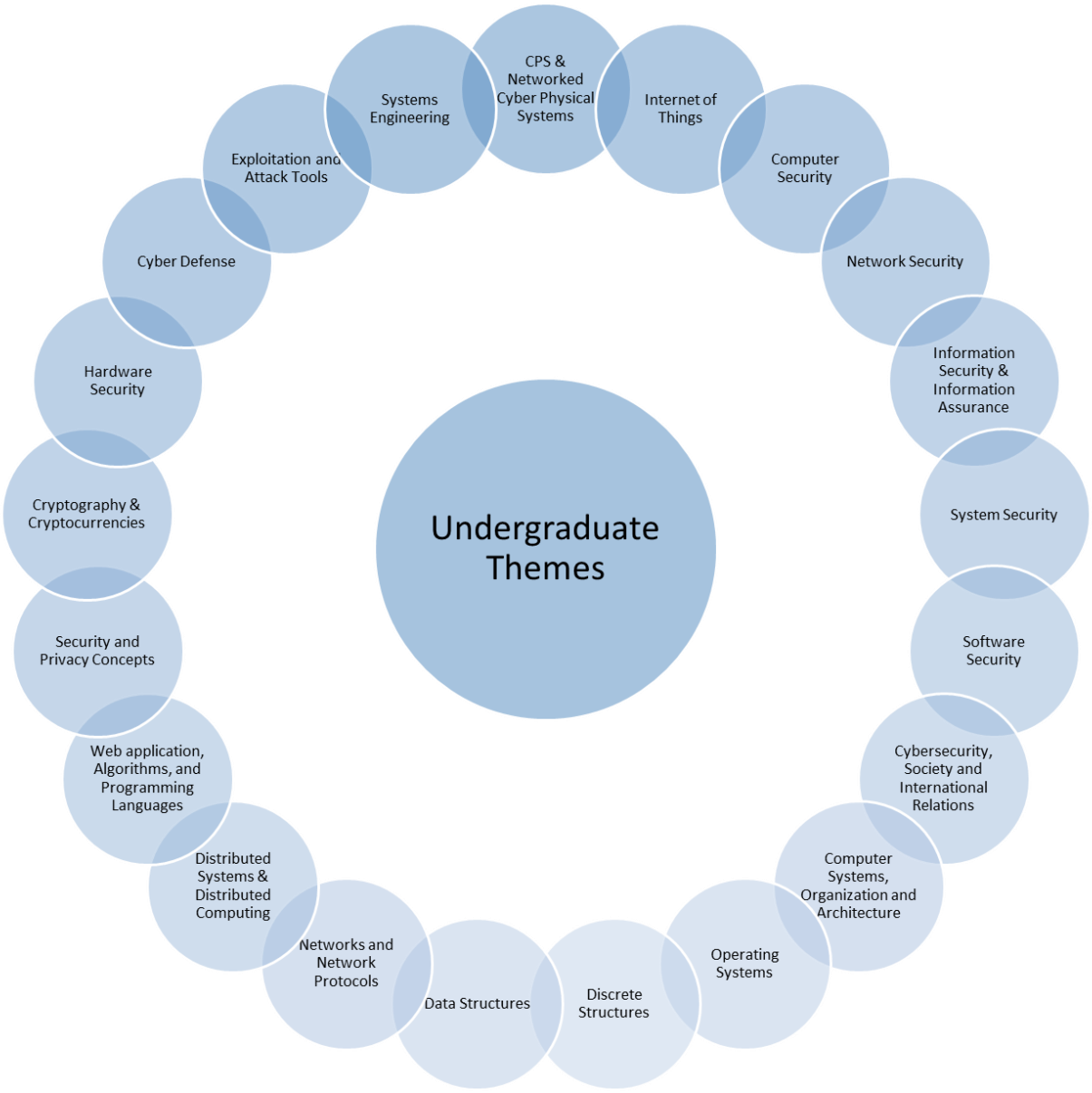

Figure 10. Undergraduate Themes

These themes represent needed skills and foundations are critical to building a workforce capable of securing our most critical systems. Unfortunately, because of the disproportionate development speed of the real-world versus academia, the reality is that few graduates are prepared to engineer CPS solutions. This leaves huge gaps in security in CPS and very few people capable of confronting the problems. This is a major security risk, and one of the many reasons that cyber threats are recognized as the biggest threat to national security [DNI, 2017]. CPS are emerging as an area of engineering with significant economic and societal implications. Major industrial sectors such as transportation, medicine, energy, defense, and information technology increasingly need a workforce capable of designing and engineering products and services that intimately combine cyber elements (computing hardware and software) and physical components and manage their interactions and impact on the physical environment. Although it is difficult to quantify the demand, a likely implication is that more CPS-capable engineers will be needed [NAS]. Students in Computer Science and Electrical and Computer Engineering are not being sufficiently exposed to these concepts of security in CPS enough to fulfil the competencies above.

3.1 WHAT SHOULD A CURRICULUM IN RESILIENT CPS INCLUDE?

Upon initially surveying the courses offered at twenty of the US's best engineering universities according to the U.S. News & World Report [USN, 2017], we noticed a stark lack of introduction to the competencies required in this field. Even more specifically, the table shows that there is a distinct lack of security focus in the engineering tracks. There are many more computer science (CS) courses addressing security than in electrical and computer engineering (ECE).

In total we surveyed 103 U.S. universities including three military academies. To collect this information, we first visited each university's website to gather their major-specific enrollment data. After getting an understanding of their class size, we browsed their degree programs offered to both undergraduates and graduates. Every website provided access to a list of their courses offered through the academic school year, whether it was through their Course Catalog in the office of the Registrar of a list of classes on a specific department's website. By analyzing course descriptions and syllabi (when available), we were able to determine whether the course covered any CPS or security competencies. If it addressed those themes in any significant way, it was listed in the chart. As for research, we started on the university's research home page and dove in from there, collecting information on groups that they fund, faculty research, and department specific research. These groups and projects were collected and reported in the chart. The research column was the hardest to report on because of the lack of streamlined organization on the university side, so there are probably a few unreported projects. All of this information helped us analyze the state of each program and identify areas of improvement using the comparative method of most similar systems, placing programs side by side to determine their weaknesses.

3.2 SURVEY SUMMARY

The presence or absence of curriculum related to these themes was collected to provide a qualitative summary of U.S. university coverage across the CPS domain. Figure 11 shows how the CPS and security related themes are distributed across university undergraduate level education. The percentages reflect the number of the 103 university course listings that reflected these themes in their information, and does not indicate whether or not these course themes are actually taught in their undergraduate programs. This graphic is just reflective of the market interest shown across the application area of resilient CPS. Just 2% of the programs listed specific courses on CPS and Networked CPS. Programs with specialization in computer security are reflected in 21% of the 103 universities, and network security in 19%. This is to be expected at the undergraduate level where introducing specialization into the course load is difficult. However it does show the emergence of CPS as a significant skills driver has not yet been addressed broadly in the U.S. university system (consistent with the NAS report).

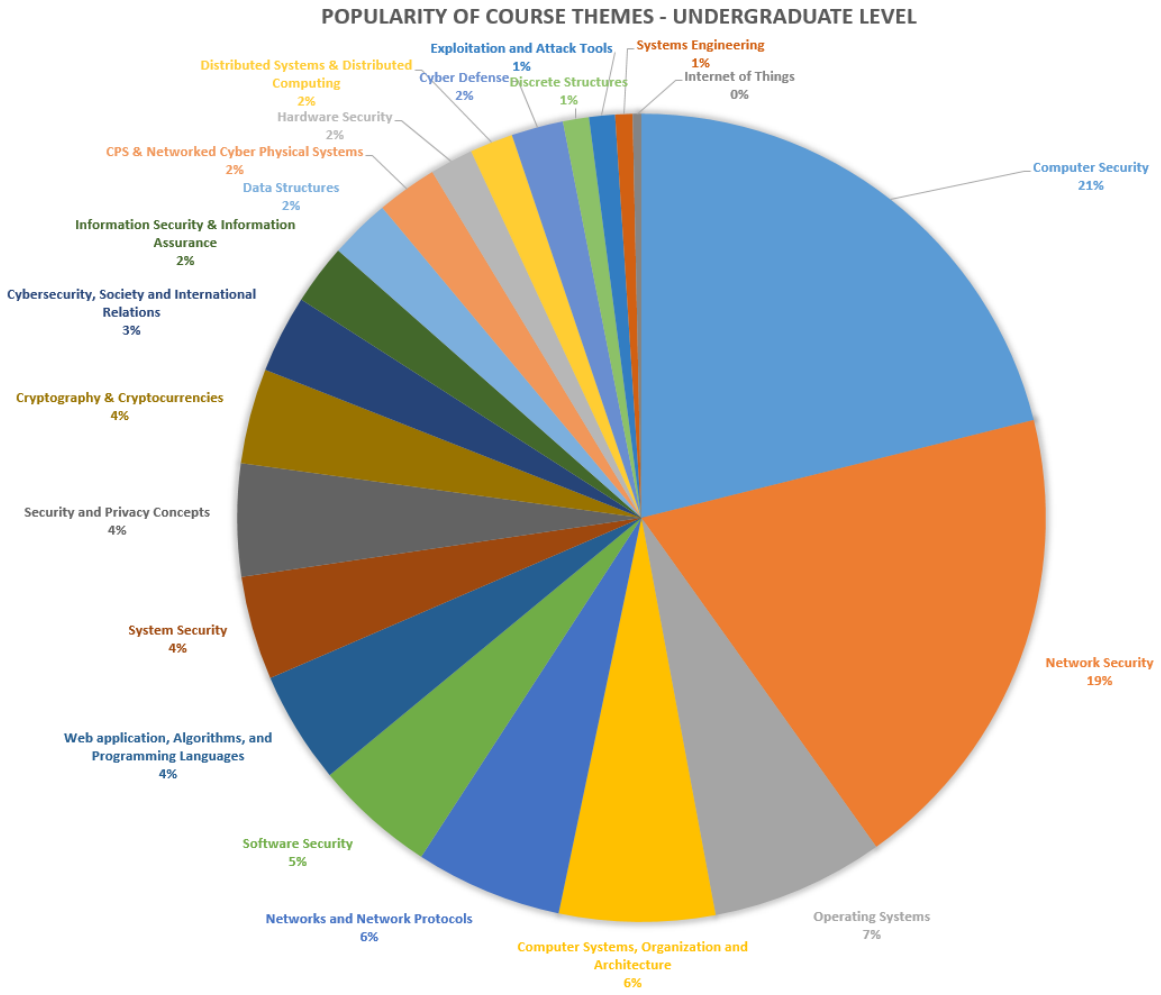

Figure 11. Popularity of Course Themes at the Undergraduate Level

Figure 12 shows how the CPS and security related themes are distributed across university graduate level education. In this set of data, 5% of university graduate programs now have CPS and Networked CPS as a course theme, and the breadth of security related topics is significantly more prevalent across the graduate curricula.

The highlighted skills and foundations are critical to building a workforce capable of securing our most critical systems. Unfortunately, because of the disproportionate development speed of the real-world versus academia, the reality is that few graduates are prepared to engineer CPS solutions. This leaves huge gaps in security in CPS and very few people capable of confronting the problems. This is a major security risk, and one of the many reasons that cyber threats are recognized as the biggest threat to national security [DNI, 2017]. CPS are emerging as an area of engineering with significant economic and societal implications. Major industrial sectors such as transportation, medicine, energy, defense, and information technology increasingly need a workforce capable of designing and engineering products and services that intimately combine cyber elements (computing hardware and software) and physical components and manage their interactions and impact on the physical environment. Although it is difficult to quantify the demand, a likely implication is that more CPS-capable engineers will be needed [NAS]. Students in Computer Science and Electrical and Computer Engineering are not being sufficiently exposed to these concepts of security in CPS enough to fulfil the competencies above. Upon surveying the courses offered at twenty of the US's best engineering universities according to the U.S. News & World Report [USN, 2017], we noticed a stark lack of introduction to the competencies required in this field. Even more specifically, the table shows that there is a distinct lack of security focus in the engineering tracks. There are many more computer science (CS) courses

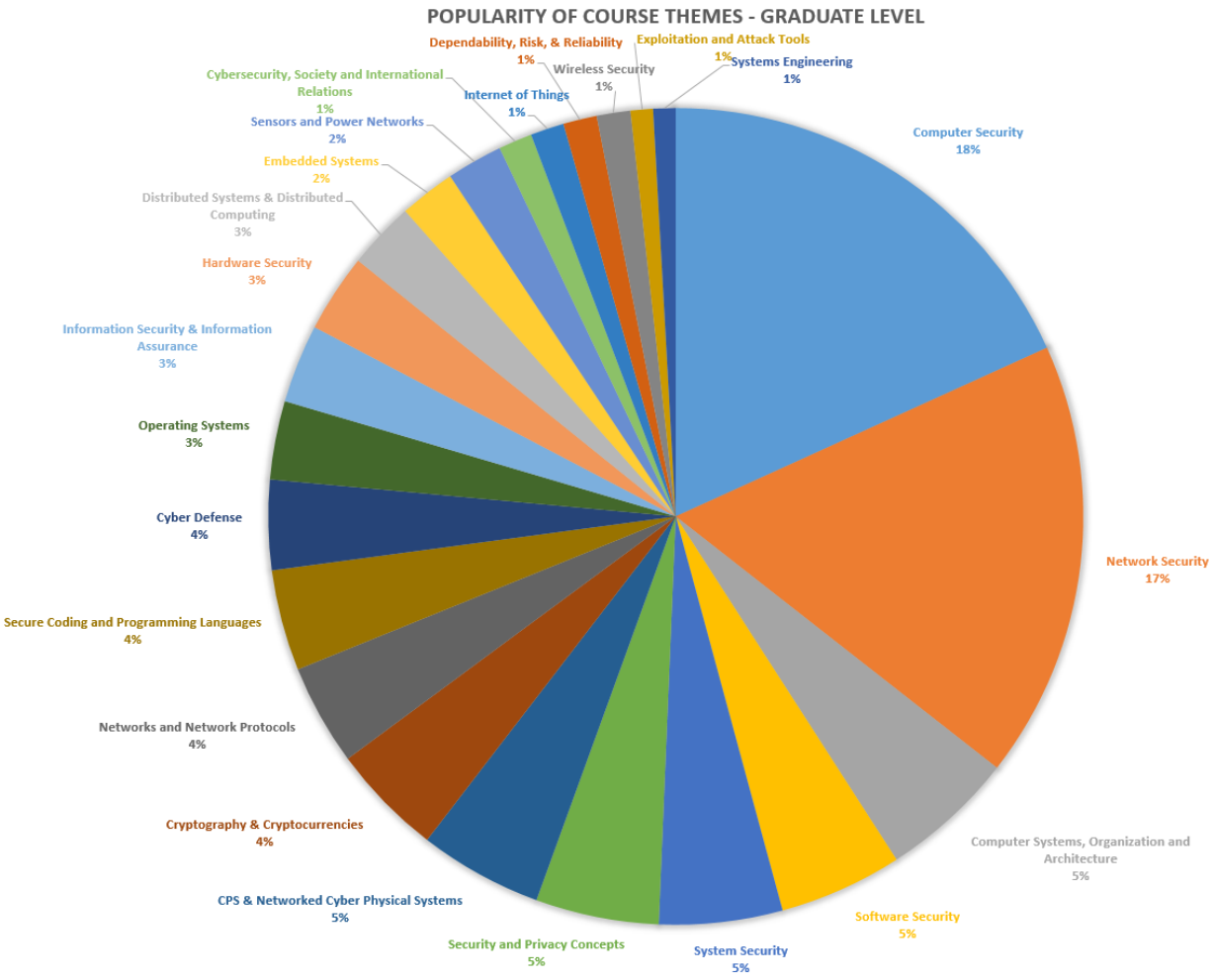

Figure 12. Popularity of Course Themes at the Graduate Level

addressing security than in electrical and computer engineering (ECE). This presents a dilemma for CPS programs considering the gap needs to be filled by students that can engineer complex solutions.

Appendix A outlines the top 20 universities and three of the US's three premier military colleges and universities their degrees offered, their courses related to cybersecurity and CPS, any advertised research/labs related to those themes, and a summary statement on their overall program status. Cryptography courses are mostly not noted in order to avoid redundancy, as every university offered an upper-division introduction to cryptography course, so they are only noted if the course stood out as one that covered more than the average program. The entire set of survey data is included as a separate report.

A summary of general findings indicates that 89 of the 103 universities surveyed offer security related courses to undergraduate and graduate students, and 89 of 103 programs support security applications in concentrations outside of the classroom via labs and projects. Figures 13 and 14 extract data from the survey associated with published security degree and certificate programs. Based on published data, 22 of the 103 universities have a dedicated security related degree, 3 at the undergraduate level and 18 at the graduate level. 16 of the 103 universities offer certificate programs with a security concentration. Only Georgia Tech, Carnegie Mellon, the University of Texas-Austin, and the U.S. Naval Academy list at this time a dedicated course on CPS. Georgia Tech and the U.S. Naval Academy list CPS Security in their course offerings.

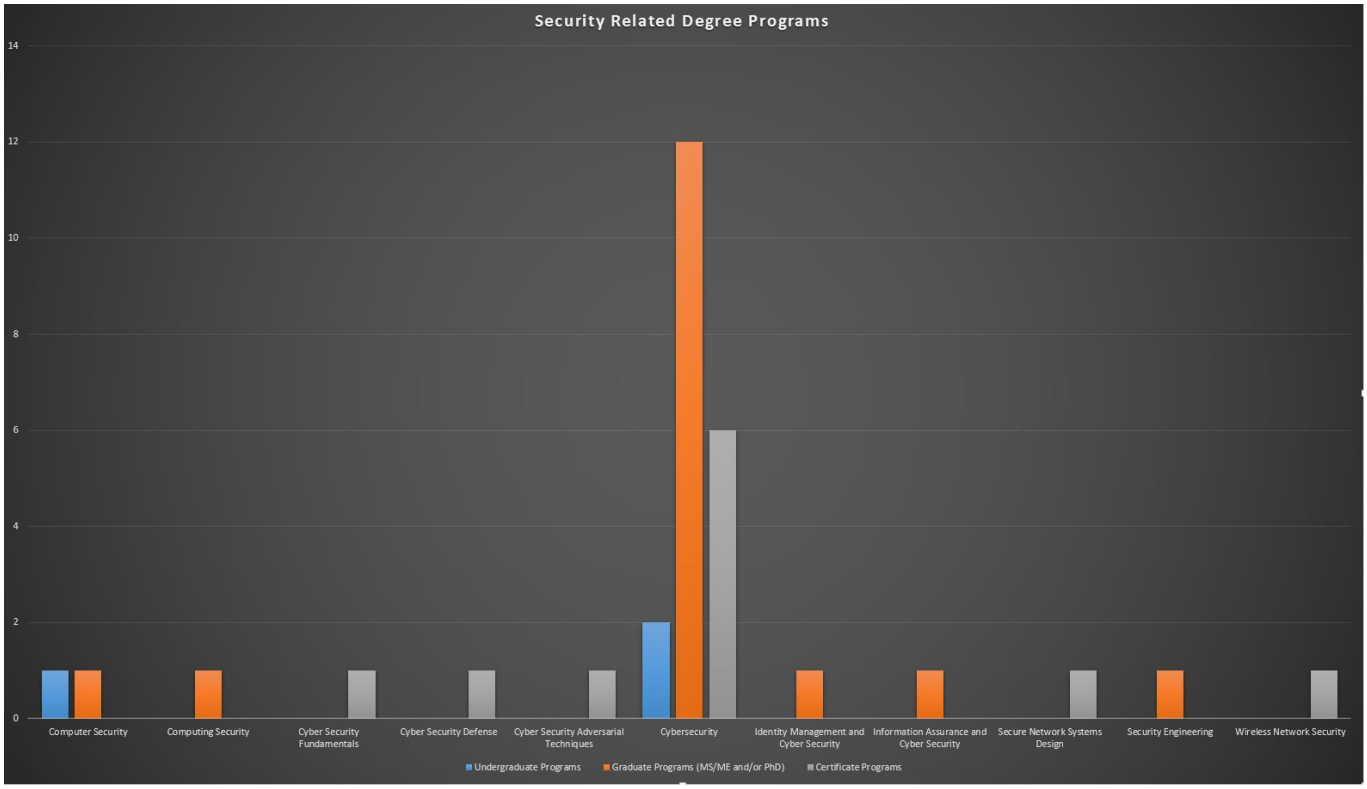

Figure 13. Degree and Certificate Programs that have a Security Related Focus

These results make apparent the lack of focus and funding CPS themes receive both inside and outside of the classroom. In many cases, like at Purdue and University of Texas, there may be efforts to address security in the classroom but a lack of attention in actual experience. This is clearly insufficient exposure to create ample knowledge of CPS security. Luckily, there are only a few cases like the University of Wisconsin and Harvard where nothing is done. There are usually at least two classes offered with a security focus at any of the schools; they tend to be a general overview of many security topics, but at least they are given some attention. The most important takeaway from the results in the taxonomy are that there are not enough course options for students to dive into security, let alone CPS, and there are even fewer opportunities to practice them in the lab. Without those opportunities, students fail to develop the skills outlined above, specifically CPS principles and concepts. Rochester Institute of Technology stands out as a place for those skills to be able to develop, specifically offering classes in security measurement, models, and methodologies. That is the level of programming that is required to fulfil the highlighted competencies. As for labs and projects, Carnegie Mellon is an example of the types of activities that need to be promoted on campuses. They address control systems threats, operating system security, efficiency of CPS, and more, giving students and faculty the chance to develop measureable skills for outside of school that directly correlate to success in CPS.

The U.S. Naval Academy probably has the most robust undergraduate program related to CPS resilience. Its list of courses might be a model for others to follow, although a military academy would be expected to have a more dedicated focus on these topics. Their courses include:

- [ECE] 310 Applications of Cyber Engineering
- [ECE] 312 Applications of Cyber Engineering for Systems Engineering
- [ECE] 356 Computer Networks with Security Applications
- [CS] 430 Computer and Network Security
- [CS] 432 Advanced Computer and Network Security
- [Cyber Science] 110 Cyber Security 1

- [Cyber Science] 202 Cyber Systems Engineering (cyber-physical system course)
- [Cyber Science] 304 Social Engineering, Hacktivism, and Information Operations in the Cyber Domain
- [Cyber Science] 308 Security Fundamental Principles

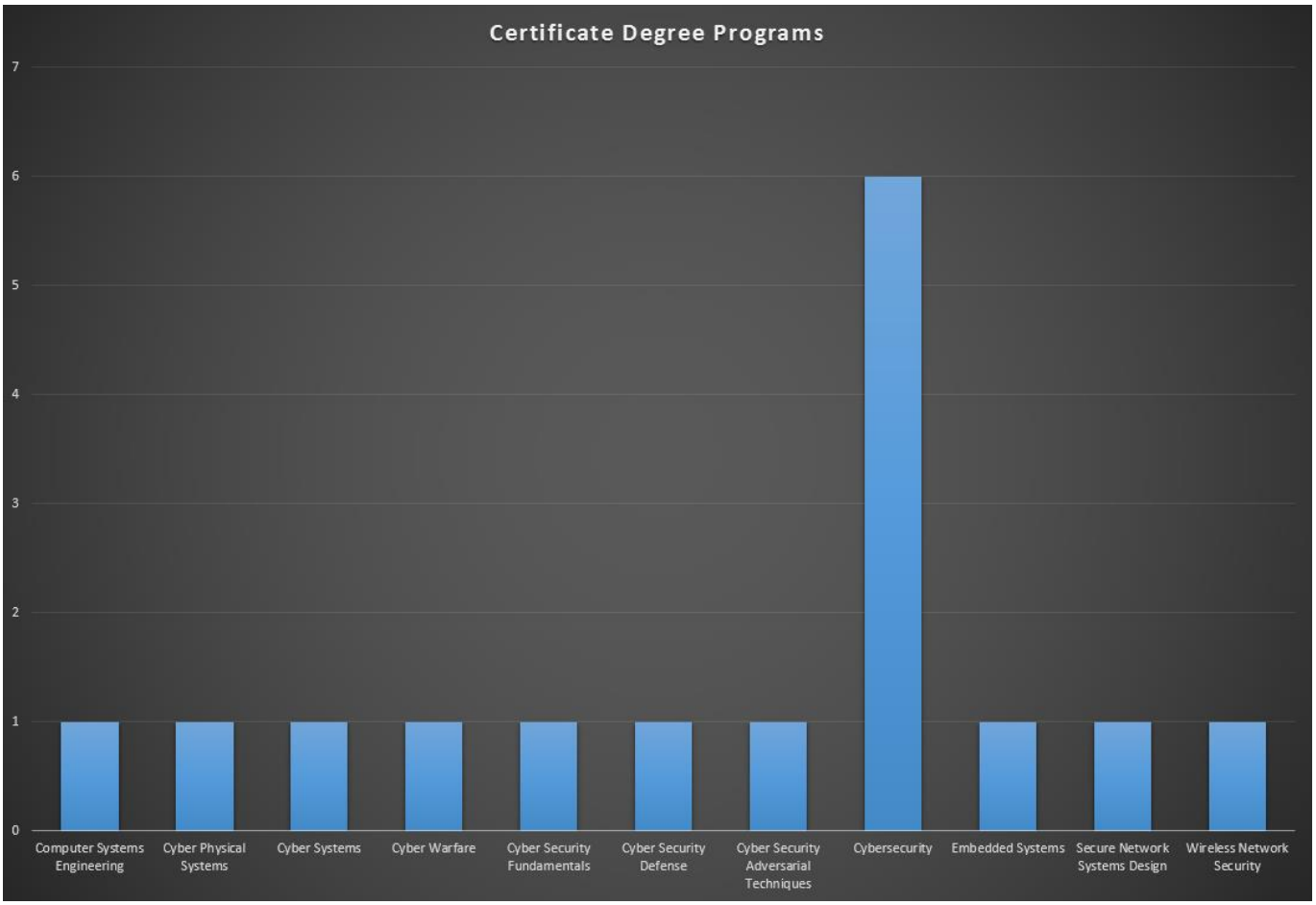

Figure 14. Certificate Programs offered with Specific Resilient CPS Topics.

Table 6 summarizes all of the results of the taxonomy development and related course themes into a single mapping. This table might be considered the start of a curriculum guide across the domain of resilient CPS. The data relates our undergraduate and graduate level course themes to the ACM Computer Engineering and Computer Science curriculum guidelines, and to the SEI assurance competencies. From this table we can see that the foundational guidance for a robust education program in resilient CPS can be created from existing foundations, with the addition of dedicated courses on CPS, CPS security, and system assurance principles. From table 6 we can also see that this type of program would be highly multidisciplinary, requiring greater interaction across engineering, computer science, and systems engineering programs than exists today. Based on the difficulty of building enough elective courses into undergraduate programs, we conclude that a fully multidisciplinary concentration on resilient CPS will be difficult to achieve without a strong pull from both government and industry.

Table 6. Themes to Curricula Mapping

Under-graduate	Graduate	Example Body of Knowledge	Example Reference Curriculum	Entry Level CPS Assurance Competencies
CPS & Networked Cyber Physical Systems	**CPS & Networked Cyber Physical Systems**	*A dedicated introductory course on CPS and a 3rd year lab on CPS platform level applications*	CE-ESY Embedded Systems CS-PD Parallel and Distributed Computing	System/software lifecycle processes System Assurance Processes System Functionality Assurance
Computer Security	Computer Security	General	CE-SEC Information Security CS-IAS Information Assurance & Security	System Assurance Processes Risk Management Concepts & Processes Assurance Assessment
Network Security	Network Security	General	CE-SEC Information Security CS-IAS Information Assurance & Security	System Assurance Processes Risk Management Concepts & Processes Assurance Assessment
Information Security & Information Assurance	Information Security & Information Assurance	General	CE-SEC-10 Trusted computing CS-IAS Information Assurance and Security	System/software lifecycle processes System Assurance Processes Risk Management Concepts & Processes Managing Assurance
System Security	System Security	Foundational Concepts; Principles of Secure Design; Threats and Attacks; Platform Security; Trusted Computing; Security Policy & Governance;	CS-IAS Information Assurance & Security CS-SDF Software Development Fundamentals CE-SEC Information Security	System/software lifecycle processes System Assurance Processes Risk Management Concepts & Processes System Operational Assurance Assurance Assessment
Software Security	Software Security	Foundational Concepts; Principles of Secure Design; Defensive Programming; Threats and Attacks; Network Security; Cryptography; Web Security; Platform Security; Security Policy & Governance; Secure Software	CS-IAS Information Assurance & Security CS-SDF Software Development Fundamentals	Software Assurance Processes Risk Management Concepts & Processes System Operational Assurance Assurance Assessment System Functionality Assurance Compliance considerations

Under-graduate	Graduate	Example Body of Knowledge	Example Reference Curriculum	Entry Level CPS Assurance Competencies
		Engineering; Software Testing & Quality		
Cybersecurity Society and International Relations	Cybersecurity Society and International Relations	Social Context; Analytical Tools; Professional Ethics; Privacy; Professional Communication; Security Policies, Laws, and Crime	CS-IAS Information Assurance & Security CS-SP Social Issues and Professional Practice	System Assurance Processes Risk Management Concepts & Processes System Operational Assurance Business Case for Assurance Managing Assurance Compliance considerations Managing Assurance
Computer Systems, Organization and Architecture	Computer Systems, Organization and Architecture	Digital Logic and Digital systems; Machine Level Data Representation; Memory System Architecture; Interfaces & Communication; Instruction set architecture; Measuring performance; Computer arithmetic; Processor organization; Peripheral subsystems; Multi/Many-core architectures; Distributed system architectures;	CE-CAO Computer Architecture and Organization CS-AR Architecture and Organization	System Operational Assurance Assurance Assessment

Under-graduate	Graduate	Example Body of Knowledge	Example Reference Curriculum	Entry Level CPS Assurance Competencies
Operating Systems	Operating Systems	Introduction to OS and OS Principles; Concurrency; Scheduling; Memory Management; Security and Protection; Device Management; Real-time and Embedded Systems; Real-time operating system design; Fault Tolerance	CE-SRM Systems Resource Management CS-OS Operating Systems	System/software lifecycle processes Software Assurance Processes Assurance Assessment System Functionality Assurance
Discrete Structures		Sets, Relations, and Functions; Basic Logic; Proof Techniques; Basics of Counting; Graphs and Trees; Discrete Probability	CS-DS Discrete Structures	System Functionality Assurance
Data Structures		Analysis Algorithmic Strategies Data Structures and Algorithms Automata, Computability, and Complexity	CE-SWD Software Design CS-AL Algorithms and Complexity	System Functionality Assurance
Networks and Network Protocols	Networks and Network Protocols	Introduction to Networks; Application of Networks; Network protocols; Network applications; Network management; Data communications; Data delivery and Reliability; Performance evaluation; Network Routing; Local Area Networks	CE-NWK Computer Networks CS-NC Networking and Communication	System Operational Assurance Assurance Assessment System Functionality Assurance Compliance considerations
Web application, Algorithms, and Programming Languages		Mobility Applications Social Networking	CS-NC Networking and Communication CS-SDF Software Development Fundamentals	Assurance Assessment Compliance considerations
Distributed Systems & Distributed Computing	Distributed Systems & Distributed Computing	IM Concepts; Database Designs; Data Modeling: Transaction Processing: Distributed Databases	CS-IM Information Management CE-SRM Systems Resource Management	System Operational Assurance System Functionality Assurance

Under-graduate	Graduate	Example Body of Knowledge	Example Reference Curriculum	Entry Level CPS Assurance Competencies
Security & Privacy Concepts	Security & Privacy Concepts	Foundational Concepts; Principles of Secure Design; HCI Foundations; Human Factors and Security	CS-IAS Information Assurance & Security CS-HCI Human Computer Interaction CS-SDF Software Development Fundamentals CE-SEC Information Security	System Assurance Processes Risk Management Concepts & Processes System Operational Assurance Business Case for Assurance
Cryptography & Crypto-currencies	Cryptography & Crypto-currencies	Cryptography	CE-SEC Information Security CS-IAS Information Assurance & Security	Risk Management Concepts and Processes
Hardware Security	Hardware Security	Resource protection models	CE-SEC Information Security	Hardware Assurance Processes Risk Management Concepts & Processes
Cyber Defense	Cyber Defense	Foundational Concepts; Principles of Secure Design; Defensive Programming; Network Security; Platform Security; Data security and integrity; Vulnerabilities and exploitation; Resource protection models; Message authentication codes; Network and web security; Authentication; Side-channel attacks; Security Policy & Governance;	CE-SEC Information Security CS-IAS Information Assurance & Security CS-SDF Software Development Fundamentals	System Assurance Processes Risk Management Concepts & Processes System Operational Assurance Assurance Assessment Concepts
Exploitation and Attack Tools	Exploitation and Attack Tools	Threats and Attacks; Digital Forensics; Security Policy & Governance	CS-IAS Information Assurance & Security	System Assurance Processes System Operational Assurance
Systems Engineering	Systems Engineering	Model-based System Design; Software Development Methods; Software Verification and Validation; Software Processes; Project Management; Tools and Environments; Requirements Engineering;	CE-SPE Systems and Project Engineering CS-SDF Software Development Fundamentals CS-SE Software Engineering	System/software lifecycle processes Risk Management Concepts & Processes System Operational Assurance Assurance Assessment Concepts Managing Assurance Compliance

Under-graduate	Graduate	Example Body of Knowledge	Example Reference Curriculum	Entry Level CPS Assurance Competencies
		Design; Lifecycle Management		considerations Managing Assurance
Internet of Things	Internet of Things	Programming Physical Systems; Resource-Aware Real-Time Computing	CS-PD Parallel and Distributed Computing	System Operational Assurance System Functionality Assurance Compliance considerations
	Secure Coding and Programming Languages	Object Oriented Programming; Functional Programming; Event-Driven and Reactive Programming;	CS-IAS Information Assurance and Security CS-PL Programming Languages	Compliance considerations
	Embedded Systems	Control Systems; Characteristics of embedded systems; Basic software techniques for embedded applications; Parallel input and output; Asynchronous and synchronous serial communication; Periodic interrupts, waveform generation, time measurement; Data acquisition, control, sensors, actuators; Implementation strategies for complex embedded systems; Mobile and networked embedded systems; Advanced input/output topics; Computing platforms for embedded systems	CE-ESY Embedded Systems	Compliance considerations

Under-graduate	Graduate	Example Body of Knowledge	Example Reference Curriculum	Entry Level CPS Assurance Competencies
	Sensors and Power Networks	Characteristics of embedded systems Data acquisition, control, sensors, actuators Mobile and networked embedded systems Computing platforms for embedded systems	CE-ESY Embedded Systems	System Operational Assurance System Functionality Assurance Compliance considerations
	Dependability Risk, & Reliability	Software Development Methods; Software Verification and Validation Software Reliability Formal Methods	CE-SWD Software Design, CE-SPE Systems and Project Engineering CS-SDF Software Development Fundamentals CS-SE Software Engineering	System/software lifecycle processes System Assurance Processes Risk Management Concepts & Processes Compliance considerations
	Wireless Security	Wireless Sensor Networks	CE-NWK Computer Networks CE-SEC Information Security CS-IAS Information Assurance & Security	System Assurance Processes Compliance considerations

3.1.1 WHAT SHOULD A CURRICULUM IN RESILIENT CPS INCLUDE?

Undergraduate and Graduate curricula for CPS specialization live at the intersection between computer engineering and computer science bodies of knowledge. The Association of Computing Machinery (ACM) provides reference curricula for both subject areas [ACM1, 2013 & ACM2, 2015]. These reports in general cover all of the knowledge areas that would be associated with CPS. What is needed is an appropriate curriculum thread or specialized degree that combined these curricula around applications of CPS. According to the NAS recommendations this should include a dedicated first year course or set of courses providing an introduction to CPS and a third year practical laboratory experience in one or more CPS platforms [NAS, 2016]. The curriculum would then include a set of foundational and principles-driven courses drawn from electrical and computer engineering and computer science domains, with practical experience in CPS applications and characteristics.

4 Part 3: Analysis of Resilient CPS Curriculum Approaches and Research Laboratory Requirements

This part of the report addresses potential high-value laboratory capabilities that would contribute to class- room based education.

There has been a general understanding that cyber security education must include teaching about the relationships between: 1) a system's vulnerabilities, 2) potential attacks against that system and their consequences and 3) possible defenses. Recently, with the advancement of automation initiatives (UAV's, autonomous vehicles, 3d printers, etc.) and the Internet of Things, recognition of the potential for cyber attacks on physical systems has grown. With that recognition, new potential consequences of cyber attacks have been illuminated, including possibilities to seriously impact safety and the control of weapon systems. Solutions to address such attacks include designing systems that include cyber security features to not only defend the system, but also to recognize successful attacks and rapidly respond so as to control consequences and enable reconfigurations that permit restarting or continuing operation. These features are categorized as part of a system's resilience. The academic community has started to address cyber-physical system security problems and system resilience, but it will require special efforts to accelerate the advancement of our nation's academic programs in this area of need. One of the major requirements for achieving accelerated outcomes, as measured by the development of related human capital, is the need for academically focused laboratories where students are exposed to the relationships between: 1) physical system designs and related vulnerabilities to cyber attacks, 2) potential cyber attacks and physical consequences, 3) possible solutions that provide needed resilience to attacks, and 4) employment of model-based engineering tools for prioritizing potential solutions.

The results of this report are based upon: 1) a survey conducted to help determine the current state and trends in academia related to the creation of laboratory capabilities for supporting cyber-physical system resilience education at the undergraduate and graduate levels, 2) a survey of laboratory designs that support ongoing academic and industry research efforts that are experimental in nature and could potentially support class room education efforts, and 3) results currently being achieved through a July 2017 initiated cyber attack resiliency education program provided by UVA to 12 members of the Defense Intelligence Agency workforce.

The remainder of this report is divided into the following sections:

- Section 2 discusses the results of the UVA survey of current cyber attack focused cyber physical system resiliency-related laboratory capabilities that academic and industrial institutions currently employ.
- Section 3, based upon the UVA experience with the DIA education effort referred to above, highlights the content of specific material that resiliency-related curriculum should include as a valuable precursor to laboratory efforts
- Section 4, based upon relevant laboratory efforts in industry and academia discussed in Section 2, highlights design concepts for laboratories that would permit the conduct of basic cyber physical system cyber security experiments that serve the educational needs of students within the bounded budgets of academia.
- Section 5, based upon the UVA experience with the DIA class, highlights the opportunity and value of including model-based engineering tools in the laboratory environments. These tools would permit students to gain hands-on experience with using systems engineering analysis tools together with cyber physical system experiments as a basis for understanding the issues of cyber attack resilience.
- Section 6 summarizes the results presented in Sections 2 through 5 and suggests possible steps forward for applying these results.

4.1 LABORATORY SURVEY RESULTS

One of the early analyses performed on this project was an assessment of the effort being made nation-wide toward the development of education-focused laboratories to support cyber-physical system (CPS) cyber security curriculum activities. To this end an initial search of available online resources was performed related to several universities and industries, some of which were also contacted directly to further discuss their specific activities on CPS security. Table 1 below identifies the university and company web sites reviewed. From the preliminary online survey, in which 30 major universities and companies were considered, the outcome showed clearly that the majority of current curriculum activities and laboratories focus on traditional information technology (IT) security, with little or no evident inclusion of cyber-physical security activities at this time. In the following text we summarize the feedback received from a few universities and companies that are working on increasing education activities on CPS security. At the University of Pennsylvania, one of the current leaders in CPS cyber-security, focus is primarily placed on research. However, a special topic course on security of embedded systems, CPS, and IoT has been offered, starting in Spring 2017. This course is organized as a seminar with presentation of papers and discussion on technologies, types of attacks, and defense methodologies. There is not a CPS security laboratory for students. However the class has a final project with hands-on hardware and simulation experiments. At MIT, the most relevant CPS security activity found is a course on resilient infrastructure networks and a workshop for CPS cyber security awareness through the use of games and demonstrations to general public audience. At the University of Illinois at Urbana Champagne, similar to the previous institutions, courses on CPS security are few and mostly focused on smart grid operations leveraging existing faculty members' research laboratories. Virginia Tech is building a CPS Security Laboratory in the Washington DC area, to bring together industry and government sponsors to address fundamental security challenges. They are collaborating with energy, automotive, embedded systems, wireless, and big data centers to create this resource.

Table 7. Reviewed University and Industry Laboratories

	Link
Virginia Tech	https://www.hume.vt.edu/cpss
University of Maryland	http://www.cyber.umd.edu
ICYPHY	https://www.icyphy.org
Duke	https://sites.duke.edu/ihss/2011/12/06/b-cyber-security/
UIUC	https://publish.illinois.edu/cps-security/
UMass	http://infosec.cs.umass.edu
Oklahoma State Un.	https://spears.okstate.edu/news/2015/05/26/oklahoma-state-university-receives-cyber-defense-education-recognition/
George Mason Un.	http://business.gmu.edu/cyber-security-degree/
UT San Antonio	http://www.utsa.edu/spotlights/cybersecurity/
Bellevue	http://www.bellevue.edu/degrees/center-for-cybersecurity-education/cce
University of Washington	https://www.pce.uw.edu/certificates/cybersecurity
Southern New Hampshire University	http://www.snhu.edu/online-degrees/bachelors/bs-in-information-technologies/cyber-security
Colorado Tech	http://www.coloradotech.edu/degrees/bachelors/cyber-security
St. John's University	http://www.stjohns.edu/academics/schools-and-colleges/college-professional-studies/programs-and-majors/cyber-security-systems-bachelor-science
UCSD	https://blink.ucsd.edu/technology/security/user-guides/security-course.html

UCSD	https://onlinedegrees.sandiego.edu/programs/master-of-science-in-cyber-security-operations-and-leadership/
UCLA	http://www.msol.ucla.edu/cyber-security-certificate/
UCLA	http://evc.ucla.edu/announcements/cybersecurity-training-for-ucla-employees
NYU	http://cybersecurity-strategy-masters.nyu.edu/?%20campaign_id=googlesearch&utm_medium=cpc&utm_source=google&utm_term=cyber%20security%20program&gclid=CjwKEAjwgtTJBRDRmd6ZtLrGyxwSJAA7Fy-hDVSr3FqJ8pcyca8SdirTXSzCYhxORzFjqJTqUD8n8RoCcS_w_wcB
BROWN	https://professional.brown.edu/cybersecurity/?gclid=CjwKEAjwgtTJBRDRmd6ZtLrGyxwSJAA7Fy-huhuWbBM4L1frAFOJXr0kXgzHcIW-76vmpLpeHOcjEBoCgnjw_wcB
HARVARD	https://www.extension.harvard.edu/academics/professional-graduate-certificates/cybersecurity-certificate?&kw=%2Bcybersecurity%20%2Bdegrees&adgroup=CERT-NT+-+Cybersecurity+-+Degree+%28b+%29&creative=101083996626&matchtype=b&network=g&adposition=1t3&target=&device=c&devicemodel=&campaign=CERT-NT+-+Cybersecurity&feeditemid=&campaignid=340841466&adgroupid=21097153626&loc_physical_ms=9008336&loc_interest_ms=&targetid=kwd-32369932479&slid=&utm_source=google&utm_medium=cpc&utm_campaign=CERT-NT+-+Cybersecurity&utm_term=%2Bcybersecurity%20%2Bdegrees&gclid=CjwKEAjwgtTJBRDRmd6ZtLrGyxwSJAA7Fy-hCBrxLtKGnN2hZdP55WsGr4CA5kg3NF7JyH46IXC0RRoCZT_w_wcB
UPenn	https://rtg.cis.upenn.edu/cis700-002/
NIST - NICE Conference	http://csrc.nist.gov/nice/2013workshop/tracks_abstracts/track2_abs/multimedia_based_virtual_classroom%20_cyber_physical_systems_security_education.html
PBS	http://www.pbs.org/wgbh/nova/labs/about-cyber-lab/educator-guide/
MIT Lincoln Lab	https://www.ll.mit.edu/mission/cybersec/cybersec.html
Honeywell	https://www.honeywellprocess.com/en-US/explore/services/industrial-it-solutions/Pages/industrial-cyber-security-lab.aspx
NetDevGroup	https://www.netdevgroup.com/content/cybersecurity/labs
University of Arizona	https://mis.eller.arizona.edu/news-article/25apr2016/cyber-security-university-arizona
Cal Poly + BHEF	http://www.bhef.com/news-events/releases/bhef-members-dedicate-innovative-cybersecurity-lab-california-polytechnic
Parsons	https://www.parsons.com/services/cybersecurity/
Vanderbilt	https://engineering.vanderbilt.edu/news/2006/vanderbilt-engineering-to-join-new-national-cyber-security-initiative/
CMU	https://cylab.cmu.edu/education/index.html
Booz-Allen Hamilton	https://www.boozallen.com/expertise/cyber.html

In general, most of the academic institutions sampled in this analysis don't yet have well-formed curriculum activities around CPS security and usually include this topic as a subset of a broader subject, either in the context of general CPS or in the context of IT security. No sharable laboratories for CPS cyber attack related resilience were found based on the institutions analyzed in this work.

Within industry, companies are starting to become more interested in CPS cyber security and are directing some of their workforce toward this area. For example, Booz-Allen Hamilton, a major IT support/consulting company in the DC area, has recently begun to transition toward CPS cyber security. As part of this initiative, they are creating in-house laboratories to train employees by addressing different security problems related to modern physical systems. Another example comes from the Honeywell Industrial Cyber Security Lab, which is an environment where Honeywell develops and tests new cyber security solutions to defend industrial control systems (ICS) and critical infrastructure from cyber-attacks. Companies, in general, seem to prefer to delegate education and laboratory activities to universities in which, for the purposes of faculty research, there may be more resources invested to create the desired laboratories. The general feedback obtained both from academic and industrial institutions is that there is a need for laboratories that will support CPS cyber security education activities, and these laboratories should be very useful for training new and current generations of students, engineers, and scientists to deal with CPS cyber security problems.

4.2 EDUCATION PRECURSORS REQUIRED TO SUPPORT RESILIENCE LABORATORY ACTIVITIES

While the purpose of this report is to illuminate the potential values of laboratory classes to support cyber attack resiliency educational curriculum, there is a corresponding need for curriculum that supports important laboratory classes. This section highlights two specific areas of knowledge that are deemed by the authors as necessary to prepare students to engage in meaningful resiliency-based laboratory efforts.

The first of these two areas of knowledge is fault tolerant systems. Approaches to achieve system resilience had been developed before cyber physical security became a design concern. In particular, techniques for achieving fault tolerance in systems have existed for several decades. Faults can occur naturally in many systems, and many applications have required continued operation in the presence of faults. Thus, a curriculum intended to address cyber security will benefit from foundational knowledge from the established area of fault tolerance. Section 3.1 below provides an overview of content within the area of fault tolerant systems that would be important for students to learn about as a precursor to engaging in laboratory efforts that explore cyber attack related security solutions. Note that Section 5 highlights the application of Attack Tree tools for assessing potential cyber attacks as a potentially high value component of a laboratory class. The attack tree tools are a derivative of more general tools used for analyzing fault tolerance solutions.

The second area covers a taxonomy consisting of a full range of attack components, that when integrated, result in a portfolio of attacks that could impact the operation of cyber physical systems. These components include attacks on information systems, network systems and physical systems that when combined can result in a physical system consequence that requires a resiliency solution. The following sections address fault tolerant system education needs and provide a cyber attack taxonomy relevant to physical system resiliency.

4.2.1 FAULT TOLERANT SYSTEMS

Agreement regarding the definitions of some common terms will help to clarify the relationship between fault tolerance and cyber physical security. Resilience is the capability of a system to recover quickly from difficulties.

Resilience and fault tolerance both address operation in the presence of faults or other difficulties. Faults can arise for many reasons including malicious actions, and techniques from fault tolerance may help to enhance resilience regardless of cause.

Fault tolerance is the ability of a system to continue operating properly in the event of a fault. When a fault occurs, the fault may be masked so that it has no further impact on system operation. If fault masking is not available or is not successful, then an error results. In a similar manner, an error may be masked so that it has no further impact on system operation. If error masking is not available or is not successful, then a failure results. A failure may also be masked so that it has no further impact on system operation, or the system may fail.

Faults may have different durations. A transient fault does not persist beyond just one event. A permanent fault persists for all time after the initial event. Intermittent faults repeat, but not continuously.

Much work related to fault tolerance assumes that there is only a single fault at a time. This assumption can be reasonable because electronic devices tend to be very reliable, and physical faults in electronics are relatively rare. If faults are assumed to arise from natural phenomena, then it is reasonable to assume that electronic devices will only experience a single fault at a time. The single fault assumption simplifies analysis and design for fault tolerance.

Nonetheless, the designer might want to consider multiple simultaneous faults. As system complexity increases, so does the probability of multiple faults. When applying the techniques of fault tolerance to cyber physical security applications, equivalent faults arise from malicious attacks rather than from natural phenomena. Malicious attacks can exploit multiple simultaneous faults.

Fault tolerance is a broad term, and there are several common measures of fault tolerance. One measure is availability, which is the probability that a system is operating correctly at a particular time. Another measure is reliability, which is the probability that a system has been operating correctly for a particular time interval. The difference between availability and reliability is subtle. Reliability is the probability that a system continues to work over an entire time interval without interruption. Availability is the probability that a system is operating correctly at a particular time, but availability allows the system to fail and be repaired. Both reliability and availability include the notion of mean time to failure (MTTF). A system that is allowed to fail and be repaired also includes the notion of mean time between failures (MTBF). The mean time between failures is the sum of the mean time to failure plus the mean time to repair (MTTR).

The notion of availability is related to the concept of resilience. Availability represents the probability that a system is operating correctly at a particular time even though the system may fail and be repaired. Resilience represents the capability to recover quickly from failure. Availability improves with improved resilience. Availability is the ratio of mean time to failure divided by mean time between failures. Alternately availability is the ratio of the mean time to failure divided by the sum of the mean time to failure plus the mean time to repair. The mean time to repair can also be viewed as the mean recovery time.

Tools are needed for design and analysis of cyber physical system security. Tools and techniques exist for design and analysis of fault-tolerant systems, and these tools may be adapted for application in the cyber physical security domain. One approach used by designers of fault-tolerant systems is fault tree analysis. Fault tree analysis has been adapted for application in cyber physical security in the form of attack trees. Basic knowledge and understanding of fault trees may help the designer to understand the application and use of attack trees.

Fault tree analysis is a deductive procedure for analysis of paths leading to failure. Central to fault tree analysis is an assumption that a system has failed in a certain way. The procedure then endeavors to deduce the modes that contribute to this particular failure. Thus, the top of a fault tree is occupied by a particular undesired event. This event typically represents a complete failure of some sort, but the top event could be chosen to represent any

particular undesired event. The choice of the top event is important because a top event that is too general may lead to analysis difficulty while a top event that is too specific may provide only a narrow view of the system. An example top event might be the crash of an airliner. A less complex top event might involve the failure of a car to start.

A fault tree model is a graphical representation of the various parallel and sequential combinations of faults that could reasonably contribute to the occurrence of the top event. Because the fault tree focuses on its top event, the tree only includes faults that contribute to this top event. This fault list is not exhaustive.

Tools exist to assist in the construction of fault trees. The trees are graphs interconnecting primary events, intermediate events, and fault tree logic gates. These places in a fault tree identify potential causes of the top event along with the ways that the sources and intermediate steps lead to the top event. The basic fault tree is qualitative in nature as it simply identifies causes and paths to the top event. Fault trees can be augmented by probabilities to support quantitative analysis. Thus, knowledge of probabilities of precursor events coupled with fault tree structure can provide the probability of top event occurrence.

The fault tree methodology provides an ordered approach for identifying the conditions that could lead to an undesirable event. Starting from the top event the approach involves a methodical enumeration of conditions that could enable the top event. In turn, these conditions are considered as events for identification of their precursor conditions. This process continues until basic events are eventually reached. If probabilities can be assigned to these basic events, then the fault tree structure enables quantitative determination of the top event probability.

Goal structuring notation (GSN) is another approach that can be useful for analysis and is commonly used to improve structure, rigor, and clarity of arguments regarding system properties. Safety critical systems such as public transportation and medical devices must be designed to assure certain levels of safety. This assurance is provided through an argument called a safety case. A safety case should communicate clear, comprehensive, and defensible arguments that a system provides an acceptable level of safety within a defined context. Similar cases could be made to provide assurance of other system properties such as security.

The challenge of an assurance case is to minimize ambiguity so as to maximize confidence. An assurance case includes several specific elements. The case must identify specific requirements and objectives. Evidence must be included to support arguments. Arguments must be made based on the provided evidence to demonstrate that requirements and objectives will be reasonably attained. Assurance cases may present their arguments using free text, but the ambiguity of free text limits the value of the assurance case. A primary purpose of goal structuring notation is to reduce ambiguity.

Goal structuring notation explicitly represents case elements and their relationships in a graphical form. Several symbols are used in this graphical notation including symbols for goals, solutions, strategies, context, and others. A goal structure may start with a top level goal supported by multiple strategies. These strategies, in turn, may involve multiple lower-level goals. Goals may also lead to solutions. The approach imposes a structure that provides greater clarity and rigor than free text.

When considering system resilience, the notion of errors within the system is difficult to avoid. A purpose of fault-tolerant design is to mask or otherwise avoid having faults become errors. A purpose of safety critical design is to ensure that faults and errors do not lead to unsafe conditions. To the extent that errors are manifestations of incorrect operation, a purpose of cyber physical security is to prevent errors arising from malicious actions from opening vulnerabilities. Thus, error detection becomes central to many notions of system assurance. A problem cannot be addressed until the problem is detected.

Redundancy can be used to check for errors at different levels. Error checking can be performed through redundant comparisons of the outputs from the lowest level components in the system. At the other extreme, redundant comparisons can be performed among the results from the highest level from input to output. Comparisons can be performed at any level between these two extremes. While error checking at the highest level can reduce hardware requirements, high-level checking typically provides only limited diagnostic information. Also, high-level checking may exhibit greater latency as an entire task must be completed before the comparison can be performed. The limited diagnostic information and greater latency of high-level checking makes recovery more complex.

Forward error recovery enables continued system operation when an error is detected by compensating for the error. This recovery requires additional redundancy beyond that which would be needed for error detection alone. For example, physical redundancy using two modules allows comparisons to detect an error but is insufficient to determine which module is correct when there is disagreement. Physical redundancy with three modules can detect an error and determine which module is wrong so that operation can continue. Faults can be masked using either extra physical hardware or extra time. Extra physical hardware can mask permanent, transient, and intermittent faults. Temporal repetition can mask some transient and intermittent faults but is typically unable to mask permanent faults.

Triple modular redundancy provides an example of forward error recovery with masking redundancy. The triple modular redundant system includes three modules that perform redundant operations. The outputs of each of these modules goes to a voter, and the voter provides an output based on a majority vote of the three inputs. Thus, a fault in one of the three processing modules will be masked by the majority vote of the two other modules.

Backward error recovery establishes known good process states as recovery points. When an error is detected, the process is rolled back to the last recorded recovery point. The process then repeats the work from the last recovery point. Backward error recovery does not mask faults and does not continue operation in the presence of faults. Rather, backward error recovery restarts processing from a known good point when a fault is detected.

Backward error recovery can yield live lock in the presence of a permanent fault. For example, the backward error recovery mechanism detects a fault and rolls the process back to the last known good recovery point. The process restarts from that recovery point and proceeds until it again encounters the same fault. The mechanism then repeats the process of rolling back to the last known good recovery point and proceeding from there. Thus, the same segment of code between the recovery point and the fault is repeated continuously.

Dynamic redundancy provides for reconfiguration of a system in response to a fault detection. For example, a primary module might be responsible for performing a particular operation. If a fault detection mechanism detects a fault in this primary module, then a standby module that performs the desired operations would replace the primary module. The standby module may be a hot standby that runs in parallel with the primary module, or the standby module may be a cold standby that is started up only when the primary module is removed to address a fault.

The triple modular redundancy example mentioned earlier could be implemented either with identical modules or with diverse modules. An error in any one module is masked by the voter as a mechanism for correcting performance from the other two modules. However, an error that arises due to the common design of identical modules will not be masked because all three modules will present identical faulty behavior. This situation arises from common cause failures. Diverse redundancy can reduce the likelihood of identical faulty behavior in the three diverse modules because diverse redundant modules are less likely to experience common cause failures.

Several different forms of diverse redundancy are possible. The U.S. Nuclear Regulatory Commission (NRC) recognizes several different types of diverse redundancy for the critical systems that they regulate. Example diversity types include: design, equipment manufacturer, logic processing equipment, function, life cycle, signal,

and the logic. Different degrees of diversity are possible within each diversity type. The NRC has established a scoring mechanism to allow the comparison of the relative diversity provided by different options within each diversity type.

The navigation system for an autonomous drone can serve to provide an example of diverse redundancy. Primary position is determined using the global positioning system (GPS). Diverse redundant position information can be provided by an inertial navigation unit (INU). Inertial navigation is subject to the accumulation of error and must be periodically corrected by the GPS. Other than that periodic synchronization, the two navigation units exhibit a few common cause failure modes. Thus, an error in one unit from any cause is unlikely to yield a corresponding error in the other unit.

Fault tolerance is a well-developed field that makes contributions to system resilience. Fault tolerance can be quantified. Redundancy is central to fault tolerance, and diverse redundancy strengthens detection and response to multiple faults. This helps to defend against natural faults and is essential for response to intentional attacks. There are many types of redundant diversity, and diversity in redundancy may be quantified.

4.2.2 CYBER ATTACK TAXONOMY FOR CYBER PHYSICAL SYSTEMS

Cyber-physical systems have become an integral and ubiquitous part of today's computing fabric. Routers, firewalls, medical devices, communications equipment, SCADA (supervisory control and data acquisition), and other industrial control systems (ICS), and autonomous vehicles are examples of cyber-physical systems that are particularly important to secure against compromise. The Department of Defense (DoD) now critically relies on cyber-physical systems for all aspects of their operations. Thus, it is of paramount importance to secure these systems from attack and compromise.

An important step towards secure cyber-physical systems is a comprehensive enumeration of the attacks that must be thwarted. Such an enumeration provides a useful resource for those who are charged with educating personnel working with critical cyber-physical systems, and it provides a useful resource for those charged with securing critical cyber-physical systems. Toward this goal, this document presents a taxonomy of cyber-physical system attacks and discusses example attacks within each category. Our intent is to be comprehensive, but one should realize that the attack space is dynamic---new attacks are continually being created. Thus, one should realize this section of the report will need constant review and update.

The remainder of this section has the following general organization. The following section presents the attack taxonomy. The following sections discuss each category and describes some attacks in the particular category. Appendix 3 provides the set of references that were considered in the development of the attack taxonomy. To discuss attacks, it is necessary to also understand, at a high-level, the flaw or vulnerability the attack is attempting to exploit. Thus, the discussion also makes use of another taxonomy—"A Taxonomy of Computer Program Security Flaws" developed by Landwehr et al.]. In particular, the Landwehr taxonomy categorizes the space of vulnerabilities or flaws by answering the following questions:

- How did the vulnerability enter the system? Was the vulnerability intentionally introduced or is it an inadvertent error?
- When did the vulnerability enter the system? Was the vulnerability introduced during the specification phase, the design phase, the implementation phase, or the manufacturing phase?
- Where in the system is the vulnerability manifest? Is the vulnerability in the hardware or software? If in the software, is it in the operating system, the compiler, a system utility, etc.

The answers to these questions can help proactively eliminate vulnerabilities as well as the deployment of defenses against attacks that attempt to exploit any remaining or currently unknown vulnerabilities (i.e., zero-day attacks).

4.2.3 CYBER-PHYSICAL SYSTEM ATTACK TAXONOMY

Figure 15 shows the possible attacks against a cyber-physical system. In this taxonomy, the attacks are categorized according to what is being exploited. One set of attacks exploit software vulnerabilities or network flawed network implementations (e.g., buffer overflow or insecure cryptographic primitive). A second category of attacks exploit physical vulnerabilities (e.g., spoof or jam GPS signals, side channel attacks, etc.) A third category of attack exploit a cyber or physical vulnerability or both.

The following subsections discuss each category of attack and give examples of each. The enumeration of attacks is by no means complete. A complete discussion of all types of attacks is beyond the scope of this report.

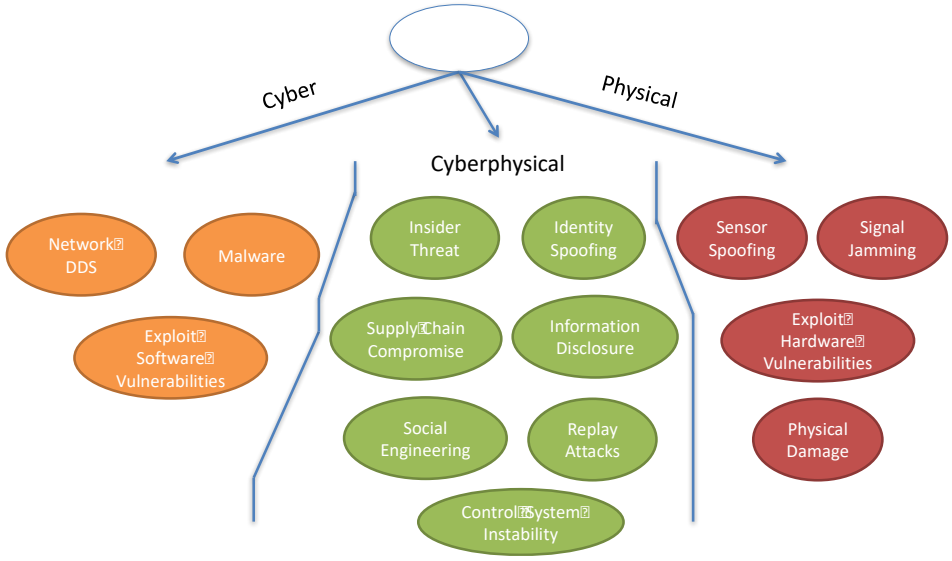

Figure 15. Cyber-physical System Taxonomy.

4.2.4 CYBER ATTACKS

4.2.4.1 Software Vulnerabilities

A major category of software attacks involves exploiting vulnerabilities present in code. These vulnerabilities appear for many reasons. A very common reason is that many cyber-physical systems run on resource-constrained devices. Consequently, software developers often favor languages such as C and C++ so they have finer control over code to meet performance requirements (execution speed and memory utilization). Unfortunately, such languages admit the possibility of programmer errors such as buffer overruns, buffer underruns, integer overflows, and unconstrained memory writes through compromised pointers. Generally, such attacks are categorized as memory corruption attacks.

A very common attack of this class exploits a buffer overrun vulnerability for a variable located on the stack to corrupt the return address. Such attacks open the possibility for hijacking control of a program to affect a remote code execution attack. By providing the appropriate input, the attacker can cause arbitrary code of their choosing to be executed on the target machine. Such attacks are sometimes referred to as remote code execution attacks.

Typically, the attacker's goal is to execute code that allows them to install malware on the target machine.

Code known as ``backdoors'' are installed. A backdoor application provides the attacker the ability to remotely log into the target machine, exfiltrate information, and compromise other connected machines.

Consider the following simple C function i

```
void bogus(void) {
  int i;
  char buffer[256];

  printf("Enter your data as a string.\n");
  scanf("%s", buffer);   // No bounds check!

  process_data(buffer);
  return;
}
```

The program accepts input from the network. The code contains a classic buffer overrun vulnerability which permits an attacker to overwrite the return address on the stack. This vulnerability is clearly illustrated in Figure 16.

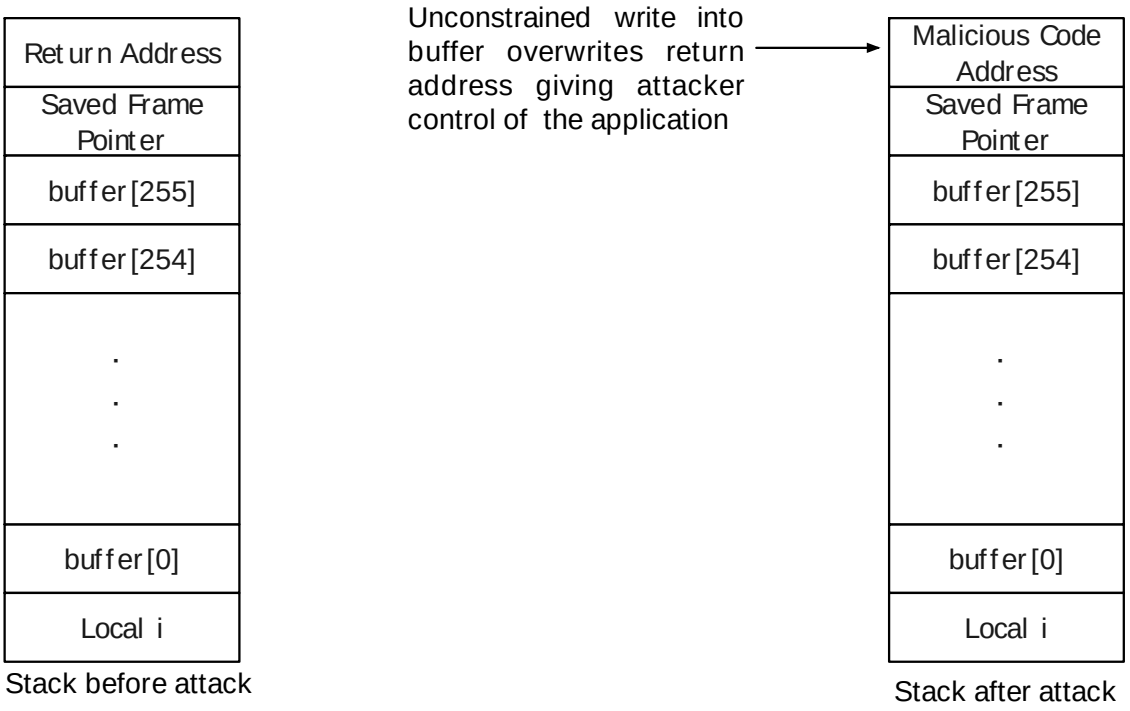

Figure 166. Stack buffer overflow vulnerability

When the proper input is sent by an attacker, instead of returning to the calling function, code of the attacker's choosing within the attacked program is executed. Kuperman et al. provide an introduction to stack buffer overflow.

Typically, vulnerabilities are unintentional. That is they are bugs that were not identified through testing or by other quality-control mechanisms. Vulnerabilities can also be intentionally placed. That is an attacker is able to compromise a piece of software during the development phase with the intent of exploiting the vulnerability once the software is widely deployed. Such attacks could also be categorized as a supply-chain attack.

Attackers are particularly resourceful at exploiting vulnerabilities and circumventing defense. For example, a popular attack that does not require code injection is the so-called return-oriented programming (ROP) attack. With ROP, an attacker is able to string together a string of code segments (called gadgets) that provide arbitrary capabilities.

Beyond memory vulnerabilities, there is a wide range of other exploitable vulnerabilities. For example, integer overflow vulnerabilities exploit the fixed precision of binary arithmetic to produce erroneous arithmetic results that cause programs to crash or have other undefined behavior. For cyber-physical systems, an effective attack may be to simply crash the application, resulting in a denial of service attack. For a cyber-physical system that is controlling a safety-critical system, such an attack, while not giving the attacker full control of the system, may be sufficient to cause substantial damage.

A different type of attack that may also result in a denial of service is one that exploits a vulnerability to consume all available resources of a particular type thereby resulting in a denial of service. For example, consider a flaw where some resource (e.g., memory, file descriptors, locks, etc.) is not returned to the free pool when they are no longer being used. An attacker could exploit the vulnerability to consume all resources thereby blocking the application from providing necessary services.

Exploitable software vulnerabilities may be in application-level software or operating system software.
It is also possible to exploit a vulnerability in hardware, although such attacks, while documented, are rare.
The sections below discuss exploitation of hardware vulnerabilities.

Malware
Another common type of cyber attack is the use of malware to compromise a machine. Such attacks typically involve human error. An unsuspecting operator receives and uses tainted media (a USB key), visits a compromised website, or is victim to a phishing attack, for example. Sophisticated malware, once installed, can quickly become stealthy making detection difficult. Preventing malware infections requires user training and careful monitoring of the integrity of systems.

Network Denial of Service (DOS)
Increasingly, cyber-physical systems are networked. Network access offers many benefits including remote monitoring, updates and data collection. Unfortunately, network access provides attackers access to the system as well as the opportunity to disrupt network operations through network denial of service attacks which essentially cut off access to the device. Depending on the cyber-physical system, network denial of service could cause disruption of service and worse. Complete failure.

Physical Attacks
Because cyber-physical systems interact with the physical world, there are a wide range of physical attacks that can be carried out. For systems that reply on sensor data, attacks that provide false sensor data, corrupt sensor data, or block the acquisition of sensor data are common.

Sensor Spoofing
With sensor spoofing, an attacker provides false sensor data. For example, autonomous vehicles rely on GPS signals to determine position and speed. Because GPS signals are relatively weak signals, spoofing or providing false sensor data can be accomplished by transmitting false data at a higher energy level.

Some autonomous systems, for example autonomous cars, acquire data through video inputs. Detecting obstacles or reading signs using video feeds is common. A knowledgeable attacker who understands the operation of the image recognition systems can provide inputs that fool the system that could result in crashes.

Also in the realm of vehicles, Shoukry et al. describe a sensor spoofing attack that compromises anti-lock braking systems.

Sensor Jamming
It is also possible to block signals through jamming. For example, GPS signals can be easily be blocked. Such an attack may not be as effective as sensor spoofing, but it still may compromise the operation of a cyber-physical system that relies on sensor data for safe and reliable operation.

Some cyber-physical systems consist of coordinating units (e.g., a convoy of vehicles, a swarm of drones, etc.).

To maintain coordination, these systems communicate with each other via RF signals. Again, an attacker may jam these signals effectively preventing the coordination necessary for safe operation (e.g., maintaining safe spacing of a convoy, coordinated maneuvers, etc.).

Hardware Vulnerabilities
Generally, it is assumed that the underlying hardware (e.g., CPU, network switches, etc.) is free from exploitable weakness for vulnerabilities. However, determined, well-funded attackers may be able to exploit hardware vulnerabilities or weaknesses.

Side channel attacks (SCAs) are powerful attacks that can circumvent even the mathematically strongest cryptographic and other theoretically strong protection mechanisms. The underlying problem is that these theoretically strong mechanisms must ultimately be implemented on concrete hardware using real software realizations of these abstract algorithms, and it is these weaker hardware and software implementations that are the focus of SCAs.

Common examples include an attacker observing the power consumption of code over time and inferring the bits of a cryptographic key (i.e., differential power analysis), reverse engineering code and then observing the timing of code execution to infer paths of execution which, in turn, reveals secret information (i.e., timing attacks), and causing cache misses or page faults to leak information.

For example, attackers who have physical access to a system can carry out a side-channel attack known as simple power analysis. By carefully monitoring the power consumption of a system, an attacker can determine a cryptographic key that provides unfettered access to a system. Many systems provide access through a master key, which is shared across devices.

Consider the implementation of RSA decryption shown in pseudo-code.

```
s=1;
while (y) {
  if (y & 1) {
    s = (s * x) mod n;
  }
  y >>= 1;
  x = (x * x) mod n;
}
return s;
```

The key observation is that a multiplication is performed when the bit in the key is 1. A knowledgeable attacker would realize that a multiplication operation would consume more power than a simple operation such as an add, subtract, or a logical operation (and, or, xor, etc.). Thus, by monitoring the power consumption when running the

code (recall for many cyber-physical systems that attacker will have access to the system), the attacker can determine the key. **Error! Reference source not found.** shows the result of a power analysis of the RSA code. The decryption key is easily discerned from the power trace.

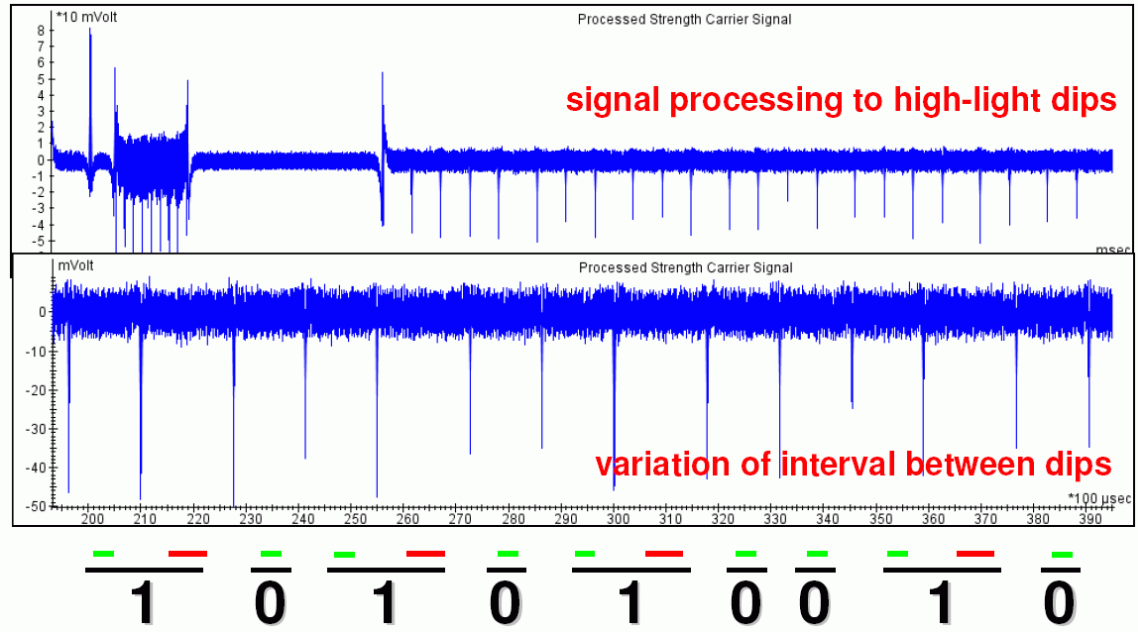

Figure 17. Power analysis side channel attack.

Beyond power analysis attacks, other side channels include timing, performance counters, page faults and cache misses.

Physical Damage

As noted in the previous section, for some systems an attacker may have physical access to the system.
Physical access opens up the possibility of physical attack. Attackers may damage sensors, actuators, pumps, and control units. Also within the realm of physical attacks is the corruption of sensor data such as applying heat or cold to a temperature sensor, physically misaligning a video sensor, etc.

4.2.5 CYBER-PHYSICAL ATTACKS

Insider Threats

According to CERT, a insider threat is “A current or former employee, contractor, or business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems.”

For cyber-physical systems, attacks by insiders can have serious consequences. Insiders may steal or modify critical, confidential, or sensitive data for personal gain for business advantage. For some cyber-physical systems (e.g., smart grid, SCADA system, smart transportation, etc.) a malicious insider can cause serious, life-threatening damage.

Identify Spoofing

For cyber-physical systems, identify spoofing is where information that appears to come from a legitimate, trusted source is actually from malicious source controlled by an attacker. Attackers can use identify spoofing to introduce a malicious node, device, or network packets into a cyber-physical system. The node can both leak valuable information or provide false information to other nodes. If the receiving node acts on the false information the

attacker can cause serious damage. Identity spoofing can be effected either by modifying identity information or by manufacturing new information.

Supply Chain Compromise
Supply chain compromise is when an attacker can introduce a flawed or vulnerable component into a system when it is being built. Software vulnerabilities can be introduced through supply chain compromise. It is also possible to introduce flawed or compromised hardware including CPUs, sensors, actuators, and other components. As should be obvious, prevention and detection of supply chain compromises is challenging.

Information Disclosure
The goal of an Information disclosure attack is to obtain information from the target system. The information targeted could be critical or private information. For example, an attacker could be sniff packets and collect information such as passwords, links to credentials, encryption keys, etc.

Information disclosure attacks are also used to determine critical system information necessary to effect other attacks. For example, an information disclosure attack might seek to learn information about the software running on a system (e.g., the software being uses, version number of the software, and patch level). This information can then be used to carry out an attack to gain control of the system.

For example, an attacker might use an information disclosure attack to learn the patch level of the software.
Once the patch level is obtained the attacker can determine if there exists a known vulnerability and exploit for the version being used. They can then use that attack to gain control of the system, disrupt operation, or corrupt information.

Another example, would be to learn the exact model and version of hardware being used. The information obtained could include the CPU type and model, sensors and actuator types and models, network interfaces, and router model, to name a few. Again, this information can be used to effect other attacks often with the goal of gaining addition privileges (i.e., privilege escalation attacks).

Social Engineering
Social engineering is non-technical attack whereby a cyber-attacker uses deception, influence, or persuasion to gain information. Social engineering attacks are most often carried out in person, over the telephone, through e-mail. Skilled “social engineers” use a variety of techniques to extract information from an unwitting person. These techniques include assuming a fake persona or role, exhibiting evidence of credibility, distraction, exploiting the innate desire to help, projecting a likable, agreeable persona, and exploiting fear.

Examples of assuming a fake persona include pretending to be a repair person, pretending to be an employee, or pretending to be a delivery person. Whatever the role assumed, the social engineer must appear credible in the role. Do they have the trappings of a repair person? Are they wearing a company uniform or clothing with a company logo? Do they provide information that makes them seem credible—dropping names of other employees, offering to have information verified by calling an office, etc.

Through distraction, a social engineer can cause people to not think clearly or carefully analyze a situation and make decisions that normally they would not make. Distraction is often used in conjunction with other social engineering techniques such as fear and the innate desire to help.

Exploitation of fear is a powerful social engineering technique. The social engineer convinces the victim that negative consequences are imminent if access or information is not provided immediately. For example, a social engineer posing as a repair person could mention that severe damage could result if they are not allowed access to

a facility to make some repair or adjustment. They implication is that it will be the other person's fault if access is not granted. The best defense against social engineering attacks is clear policies and continuous training.

Replay Attacks

Many cyber-systems have defenses in place to detect anomalous inputs or deviations from typical behavior. To avoid detection by intrusion detection and other monitoring systems, attackers can make use of replay attacks. Here an attacker is, through perhaps information disclosure attacks, is able to record normal inputs (possibly both data and control inputs) to a system for some period of time. The attacker then modifies the inputs to incorporate the false data and then replays the modified data as inputs to the victim system.

Control System Instability

A decidedly unique attack against a cyber-physical system is a control system instability attack. Here the attacker is seeing to move the control system from a region of stability to instability where control outputs may fluctuate arbitrarily and exceed normal operating parameters. The instability can cause the system to crash, produce erroneous control signals, or wildly fluctuating signals which could do physical damage (e.g., a pump cycling on and off rapidly, a valve opening and closing rapidly, an electrical component power cycling rapidly, etc.) To affect a control instability attack, the attacker may use a replay attack, sensor spoofing, or selective sensor jamming to affect the inputs to the system.

4.2.6 SUMMARY

Because cyber-physical systems consist of both cyber and physical systems, the attack surface, when compared, to either cyber or physical systems solely, is much larger. All of the attacks that apply to either apply to cyber-physical systems, but there are now combinations of attack that are possible. For example, carrying out a simple physical attack may open a vulnerability that then allows a much more serious or consequential cyber attack. Because cyber-physical systems often control major physical infrastructure, the consequences of an attacks against cyber-physical system can be catastrophic. Thus, understanding the nature of attacks and their source is of the highest importance.

4.3 LABORATORY DESIGN CONCEPTS

In this section, we discuss the design concepts for a sharable technology-design and evaluation laboratory on CPS cyber-security. Section 5 introduces analysis-focused elements into the laboratory concept, complementing the suggestions presented in this section. For the technology focused portion of desirable laboratories, the major challenges considered were related to making them: 1) as complete and realistic as possible and 2) sharable and accessible to a large audience both in- and out-side the university. To this end, we were inspired by the Robotarium at Georgia Tech (https://www.robotarium.gatech.edu) which conceptually offers similar capabilities as the ones being considered in UVA's envisioned CPS security laboratory environment. Other than GaTech's and UVA's shared laboratory concepts, no other institution that we looked indicated current activity focused on developing sharable cyber security-related laboratories for CPS. The Robotarium is a shared experimental environment for multi-robot operation. The physical environment, housed at a Georgia Tech facility, is accessible through a web interface. Users outside the university can reserve a time slot and upload their software, which will run on real ground robots within a defined space at Georgia Tech. Users will obtain data and videos as feedback.

Based on the Robotarium architecture and the analysis that UVA performed in this project, here we provide design recommendations for a sharable CPS Security laboratory:

- A CPS features a tight integration of communication, sensing, and computation with the physical world. A typical CPS contains multiple buses/networks that connect sensors and actuators with controllers, data storage and processing units, and human machine interfaces. More precisely, it consists of: a) controllers, b) networking devices and buses, c) sensors, s) actuators, and d) the physical plant. An attacker can

compromise the operation of a CPS by attacking any of these components. When building a laboratory space, it is necessary to consider one or more complete relevant and general CPS scenarios with clear interfaces to enable research and studies on different attack surfaces.

- It is necessary to provide both attack and resilience capabilities to allow a user to test different algorithms on multiple types of attacks and CPS surfaces.
- Existing, well-known attack vectors should be included within the architecture. Sensor spoofing for example can be performed in many different ways. A user that is interested in working on such problems may not be interested in focusing on the device used by the attacker to compromise the sensor. Thus, we can think of including a module that simulate and emulate the behavior of sensor spoofing.
- Since a broad audience with different expertise will have access to the desired laboratory, we recommend that the laboratory should support different levels of attack scenarios from i) simple case studies in which a user can work on a graphical interface, change some predefined parameters, and run predefined attacks for analysis purposes to ii) more complicated cases in which a user can create his or her own attack vectors and design and code resilient estimators and controllers.
- The recommended architecture for such a laboratory should consists of hardware-in-the-loop simulators in which the physical systems is connected to one or more computers exchanging information and interfaced with a network of sensors and controllers and with the external World through a web interface.
- The recommended platforms that we believe are relevant and representative of CPS applications are: unmanned aerial vehicles or drones, autonomous vehicles, and industrial control systems. For the DoD, hypothetical weapon systems could be incorporated into the laboratory environment (See Section 5). We recommend such CPS's because they consist on multiple computers, bus networks, sensors, and actuators capabilities and because they present diverse and complementary dynamics. Such systems can fit within a confined space by scaling them down to leaving the minimum representative features found on the real systems. Drones can be caged or tethered to confine their operating environment or connected to a hardware-in-the-loop setting in which only the motors are run and the rest of information are simulated on a computer. Autonomous vehicles in the form of small unmanned ground vehicles with the same sensing capabilities available on autonomous cars can be found in most modern robotics laboratories, and thus could be deployed in a confined laboratory space to enable automation capabilities such as go-to-goal, cruise control, and obstacle avoidance. The laboratory space can be equipped with multiple sensors, actuators, and programmable logic control units interfaced with computers and the unmanned vehicles described above, to create industrial system configurations, sensor networks, IoT operations, and vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) environments.
- The aforementioned platforms and the laboratory hardware and software environments should be modular to enable component swapping and inclusion of new sensors, communication, and computation capabilities, as needed.
- The CPS platforms need to be remotely interfaced and accessible via web browsers or a cloud-based environment. Thus, it is necessary to define what inputs and outputs will be available to a user that is connecting to the experimental system.
- It is necessary to consider safety. A framework to overwrite any unsafe situation and reset the system needs to be in place. In addition to concerns regarding human safety in the laboratory, it is important to avoid overrunning and possibly damaging motors, CPUs, and sensors. To this end, a supervisory control subsystem running locally inside the laboratory, decoupled from user interfaces, should be designed and deployed to monitor safety critical conditions and intervene should certain critical events occur.

- Similar to the Robotarium setup, it is recommended to build a software simulator to run first operations in a virtual environment and then transition to hardware experiments. Such a simulator provides the benefits of minimizing debugging time and unproductive experimental time.

4.4 INTEGRATING MODEL-BASED ANALYSIS TOOLS INTO THE LABORATORY EXPERIENCE

In July 2017, UVA initiated a cyber resiliency education program with the DIA. The curriculum consists of 2 courses, each containing nine 2-hour class sessions. The curriculum is attached in Appendix 1. The first course has been completed. The second course is in progress. The student body consists of 12 students with an estimated 10-15 years of systems engineering and analysis experience. Three 2-hour laboratory sessions are part of the curriculum, providing the opportunity for students to gain hands-on experience as they learn about cyber attack resilience related to cyber physical systems. This DIA class was the initial version of a potentially reusable UVA cyber resiliency professional education program and our premonition was that we'd devote the three laboratory classes to design of attacks and corresponding solutions, using system emulators (as suggested in Section 4) as the targets for prototyped attacks and solutions. However, as the initial class lectures proceeded, it became clear that the students were also very interested in utilizing off-the-shelf analysis tools that they were exposed to in the classroom lectures. SysML and Attack Tree based tools, as discussed in class, could be used to support decisions regarding which attacks to prepare for and what resiliency solutions were needed. Strong student interest with regard to both resilience-related technology and analysis pointed toward expanding our laboratory concept to include hands-on use of an available analysis tool. Since the classroom lectures would be addressing fault tolerant system design and analysis approaches, a cyber attack taxonomy, and a specific attack analysis tool (SecurITree), it was decided *with* the class to expose them to applying SecurITree to the physical system that would also be addressed as part of the laboratory activity. SecurITree is designed to help a system analyst to assess possible attack paths accounting for a variety of factors determined by the analyst, such as the capabilities of adversaries, historical attacks, system design and vulnerabilities, and attack consequences. The plan was to organize four teams comprised of three students each, to separately address a common system and then compare and discuss the differences between the prioritized outcomes of the four teams. The 3-student teams would consist of a student most interested in physical system experiments, a 2nd student most interested in using model-based tools (in this case SecurITree) and a 3rd student most interested in organizing the fundamental analysis that SecurITree would use in prioritizing potential solutions. This decision required UVA to develop a realistic, but relatively simple system use case to serve both physical system experiments and analysis purposes. This was accomplished by developing a mocked-up prototype of the control subsystem for a hypothetical weapon system that related to actual military systems, and a corresponding UVA-developed system description (operational and technical) to support analysis efforts. Documentation of the hypothetical weapon system system's description and the corresponding physical prototype are included in Appendix 2. The students were very interested in evaluating, based upon their experience, the reality of the use case, and also were interested in having the opportunity to suggest modifications that would increase the educational value of the use UVA has set up a process that will respond to this student recommendation, but at this time it is too early to determine the value of this suggestion.

UVA was able to get agreement from AMANZA, the company that provides SecurITree to use 18 licenses (6 for class room use, 12 for student home use) for 90 days. Results of the laboratory exercise will be available in December. However, based upon the first two laboratory classes, it can be reported now that student learning and enthusiasm is significant.

4.5 SUMMARY OF RESULTS AND RECOMMENDATIONS

The major outcomes from this research effort are:

1. Very few academic institutions are currently supporting cyber security related laboratories that would support educational curriculum focused on resilience of cyber physical systems.
2. However, advanced efforts in academia and industry related to cyber attack resilience for physical systems are starting to emerge, including the use of laboratories to provide experimental results. These laboratory designs offer design opportunities for new laboratories that are focused on supporting educational needs. They will need to include use of open-source and off-the-shelf software that will serve to bound the costs associated with these laboratories.
3. However, due to issues associated with DoD information security sensitivities and industry proprietary solution sensitivities, appropriate use cases for new educational-focused laboratories will need to be developed. These use cases will need to be sufficiently realistic so as to gain confidence that they usefully contribute to the education of students.
4. Resilience-focused solutions will demand future system designers who integrate solutions that are based upon technical and operational areas of knowledge that are not traditionally part of the cyber security curriculums that are now offered. In particular, techniques related to fault tolerant system design and understanding of attack taxonomies that integrate IT system attacks combined with physical control system attacks are typically not part of a cyber security-related curriculum.
5. Model-based engineering techniques provide a significant opportunity for design and evaluation of potential resilience solutions. Laboratory efforts should include physical system mock-ups for teaching about design of attacks and resilience solutions, and also include use of model-based tools for evaluating potential solutions. Use of the same physical system use case(s) for these two purposes would provide students with a greater understanding of the engineering efforts required to both derive and evaluate possible solutions.
6. Regarding model-based engineering techniques, students in UVA's DIA-sponsored educational program suggested, based on their experience, allowing them to suggest modifications to the use case scenarios that could be immediately implemented by UVA so as to add realism. This suggestion is being addressed and an assessment of its value and practicality will be determined in December, upon the completion of the educational program.
7. The resilience of physical systems to cyber attacks is a subject that is emerging at a rapid rate. Given the variety of skills and experiences required for addressing this topic, it is likely that the initial sets of students will be grouped into integrated classes and will have a diverse set of knowledge and job-related interests to build upon. As a result, the educational programs and corresponding laboratory activities must be designed to support this diversity. UVA's DIA educational program provided a first experience for addressing this issue, including discussions with the students regarding how best to respond to this challenge. Our first approach, to develop three person laboratory teams consisting of technology focused, analysis focused, and tool using focused students is currently in progress, and results will be determined in December, upon the completion of the educational program.

Based upon these results it is recommended that the DoD consider establishing one or two new cyber physical system resilience education efforts that build upon the GaTech/UVA study outcomes and include the desire to continue to gather information about these efforts that will help to identify improvement opportunities based upon actual experience.

5 Recommendations and Next Steps

In order to fulfill the discussed competencies and be ready to employ CPS skills in real time, curriculums need to be developed that diverge from the average school's Computer Science path. Further research is needed to define research challenges and related body of knowledge for resilient cyber-physical systems as well as proposed reference curriculum related to specialization in the systems engineering domain. Broader recommendations for a general curriculum in resilient computing systems are also needed. Further research opportunities exist to evaluate approaches for laboratory facility development or lab resource sharing initiatives that could address this area. The future CPS workforce needs to include a combination of engineers trained in foundational fields (such as electrical and computing engineering, mechanical engineering, systems engineering, and computer science), engineers trained in specific applied engineering fields (such as aerospace and civil engineering), and CPS engineers, who focus on the knowledge and skills spanning cyber technology and physical systems that operate in the physical world. This means that these top engineering programs can build on their pre-existing foundations, considering they will need to be utilized in building capable engineers; however, they have to go on to include CPS themes that enable graduates to confront security and dependability challenges.

Outside of the classroom, additional funding and attention must be delegated to research and projects in CPS. As with all engineering fields, this is the only way to effectively engage with these concepts and become a qualified employee in the field. CPS is a quickly emerging innovation in many different areas of our world, and it is critically important to understand how to secure them in real-time. Outside of projects with the actual application of those skills, more research into CPS security and reliability must occur in these lab environments. They area a rapidly advancing technology with little understanding of how to ensure resilience, so further research should be encouraged where the resources are available. As highlighted in Part 3 of this report, students need to be exposed to CPS themed relationships outside of their CPS classes if they intend to fulfill the discussed competencies.

Advanced efforts in academia and industry related to cyber-attack resilience for physical systems are starting to emerge, including the use of laboratories to provide experimental results. These laboratory designs offer design opportunities for new laboratories that are focused on supporting educational needs. However, due to issues associated with DoD information security sensitivities and industry proprietary solution sensitivities, appropriate use cases for new educational-focused laboratories will need to be developed. These use cases will need to be sufficiently realistic so as to gain confidence that they usefully contribute to the education of students. Resilience-focused solutions will demand future system designers who integrate solutions that are based upon technical and operational areas of knowledge that are not traditionally part of the cybersecurity curriculums that are now offered. In particular, techniques related to fault tolerant system design and understanding of attack taxonomies that integrate IT system attacks combined with control physical control system attacks are typically not part of a cybersecurity-related curriculum.

Model-based engineering techniques provide a significant opportunity for design and evaluation of potential resilience solutions. Laboratory efforts should include physical system mock-ups for teaching about design of attacks and resilience solutions, and also include use of model-based tools for evaluating potential solutions. Use of common physical system use case(s) for these two purposes would provide students with a greater understanding of the engineering efforts required to both derive and evaluate possible solutions. Regarding model-based engineering techniques, students in UVA's DIA-sponsored educational program suggested, based on their experience, allowing them to suggest modifications to the use case scenarios that could be immediately implemented by UVA so as to add realism. This suggestion is being addressed and an assessment of its value and practicality will be determined in December, upon the completion of the educational program.

The resilience of physical systems to cyber attacks is a subject that is emerging at a rapid rate. Given the variety of skills and experiences required for addressing this topic, it is likely that the initial sets of students grouped into integrated class will have a diverse set of knowledge and job-related interests to build upon. As a result, the educational programs and corresponding laboratory activities must be designed to support this diversity. UVA's DIA educational program provided a first experience for addressing this issue, including discussions with the students regarding how best to respond to this challenge.

Based upon these results it is recommended that the DoD consider establishing one or two new cyber physical system resilience education efforts that build upon the GaTech/UVA study outcomes and include the desire to continue to gather information about these efforts that will help to identify improvement opportunities based upon actual experience.

There is an impressive and competitive foundation of engineering coursework and ideals at all of these universities, so the starting point is not blank. However, the surveys above clearly show the deficit in CPS education and application opportunities for undergraduates and graduates. Program directors need to be encouraged to make major additions to their current offerings, or else we face an incredible security problem with few knowledgeable people to solve it. With the encouragement of the DoD and further research to back it, these changes will be incredibly valuable to security institutions.

6 Abbreviations and Acronyms

ACM	Association of Computing Machinery
ASD	Assistant Secretary of Defense
CPS	Cyber-Physical System
CPU	Central Processing Unit
CS	Computer Science
DoD	Department of Defense
ECE	Electrical and Computer Engineering
GPS	Global Positioning System
GT	Georgia Institute of Technology
INCOSE	International Council on Systems Engineering
INU	Inertial Navigation Unit
ICS	Industrial Control System
IoT	Internet of Things
IT	Information Technology
M2M	Machine-to-Machine
NAS	National Academy of Sciences
SCADA	Supervising Control and Data Acquisition
SERC	Systems Engineering Research Center
SoS	System of Systems
SE	Systems Engineering
SysML	System Modeling Language
UVA	University of Virginia

7 References

Executive Summary and Introduction

1. Bodeau, D., Graubart, R.,Heinbockel, W., and Laderman, E., "Cyber Resiliency Engineering Aid – The Updated Cyber Resiliency Engineering Framework and Guidance on Applying Cyber Resiliency Techniques," Mitre Corporation, May 2015.
2. National Academies of Sciences, Engineering, and Medicine (2016). A 21st Century Cyber-Physical Systems Education. Washington, DC: The National Academies Press. doi:10.17226/23686.

Part 1

3. Association of Computing Machinery, Joint Task Force on Computing Curricula, Computer Science Curricula 2013, Curriculum Guidelines for Undergraduate Degree Programs in Computer Science, December 2013.
4. Association of Computing Machinery, Joint Task Force on Computing Curricula, Computer Engineering Curricula 2016, Curriculum Guidelines for Undergraduate Degree Programs in Computer Engineering, Interim curriculum report, October 2015.
5. Avižienis, A., Laprie, J., Randell, B., and Landwehr, C., (2004) "Basic Concepts and Taxonomy of Dependable and Secure Computing," IEEE Transactions on Dependable and Secure Computing: 1(1), 11-22.
6. Boehm, B. and Nupul, K. (2015), "An Initial Ontology for System Qualities," 25th Annual INCOSE International Symposium (IS2015), July 2015.
7. "Cyber-Physical Systems." Cyber-Physical Systems. UC Regents, 2012. Web. 1 June 2017.
8. Department of Defense Instruction (DoDI) 8500.01, Cybersecurity, March 14, 2014.
9. Framework for Cyber-Physical Systems Release 1.0: Cyber Physical Systems Public Working Group (Rep.). (2016). NIST.
10. Hilbum, Thomas, Mark Ardis, Glenn Johnson, Andrew Kornecki, and Nancy R. Mead. Software Competency Model. Tech. no. CMU/SEI-2013-TN-004. N.p.: Carnegie Mellon U, n.d. Print.
11. Holtzman, D., "Cyber Resiliency Office for Weapon Systems (CROWS)," National Defense Industries Association Workshop on Resilient Cyber Weapon Systems, McLean VA, April 2017.
12. Mead, Nancy R., et al. Software Assurance Curriculum Project, Volume I: Master of Software Assurance Reference Curriculum (CMU/SEI-2010-TR-005). Software Engineering Institute, Carnegie Mellon University, 2010. http://www.sei.cmu.edu/library/abstracts/reports/10tr005.cfm
13. Mead, Nancy R.; Hawthorne, Elizabeth K.; & Ardis, Mark. Software Assurance Curriculum Project, Volume IV: Community College Education (CMU/SEI-2011-TR-017). Software Engineering Institute, Carnegie Mellon University, 2011. http://www.sei.cmu.edu/library/abstracts/reports/11tr017.cfm
14. Mead, Nancy R.; Hilburn, Thomas B.; & Linger, Richard C. Software Assurance Curriculum Project, Volume II: Undergraduate Course Outlines (CMU/SEI-2010-TR-019). Software Engineering Institute, Carnegie Mellon University, 2010. http://www.sei.cmu.edu/library/abstracts/reports/10tr019.cfm CMU/SEI-2013-TN-004 | 33
15. National Science Foundation, 2016, "Cyber-Physical Systems," program solicitation 16-549, NSF document number nsf16549, March 4. https://www.nsf.gov/publications/pub_summ.jsp?ods_key=nsf16549 .
16. Prem Jörg Irran, E., Sawyer, M., Parsons, M., Zsigri, C., Morgan, I., & Stewart, A. (2014). Next Generation Computing Roadmap (Rep.). Brussels: European Union. doi:10.2759/4587

17. Reed, M., "DoD Strategy for Cyber Resilient Weapon Systems," National Defense Industries Association, Annual Systems Engineering Conference, Alexandria VA, October 2016.
18. ReSIST: Resilience for Survivability in IST, A European Network of Excellence, Deliverable D37: Resilient Computing Curriculum, Contract Number: 026764, December 2008. Retrieved from: http://www.resist-noe.org/outcomes/outcomes.html.
19. Simoncini, L. (2010), "Technological and Educational Challenges of Resilient Computing," International Journal of Adaptive, Resilient and Autonomic Systems: 1(1), 41-57.
20. Simoncini, Luca, "Technological and Educational Challenges of Resilient Computing," International Journal of Adaptive, Resilient and Autonomic Systems (IJARAS), 1(1) 2010, pp. 41-57. DOI:10.4018/jaras.2010071703.

Part 2

21. "Best Undergraduate Engineering Programs Rankings" US News & World Report. U.S. News & World Report LP, 2017. Web. 13 June 2017.
22. Worldwide Threat Assessment of the US Intelligence Community, 2017. United States of America. Senate Select Committee of Intelligence. Office of the Director of National Intelligence. Worldwide Threat Assessment of the US Intelligence Community. By Daniel R. Coats. N.p.: n.p., 2017. Print.

Part 3

23. H. Bao, R. Lu, B. Li, and R. Deng. Blithe: Behavior rule-based insider threat detection for smart grid. IEEE Internet of Things Journa*l*, 3(2):190–205, April 2016.
24. Dawn M Cappelli, Andrew P Moore, and Randall F Trzeciak. *The CERT guide to insider threats: how to prevent, detect, and respond to information technology crimes (Theft, Sabotage, Fraud)*. Addison-Wesley, 2012.
25. A. A. Cardenas, S. Amin, and S. Sastry. Secure control: Towards survivable cyberphysical systems. In 2008 *The 28th International Conference on Distributed Computing Systems Workshops*, pages 495–500, June 2008.
26. Qian Ge, Yuval Yarom, David Cock, and Gernot Heiser. A survey of microarchitectural timing attacks and countermeasures on contemporary hardware. *Journal of Cryptographic Engineering*, pages 1–27, 2017.
27. R. Hund, C. Willems, and T. Holz. Practical timing side channel attacks against kernel space aslr. In *Proceedings of the 2013 IEEE Symposium on Security and Privacy*, SP '13, pages 191–205, Washington, DC, USA, May 2013. IEEE Computer Society.
28. Benjamin A. Kuperman, Carla E. Brodley, Hilmi Ozdoganoglu, T. N. Vijaykumar, and Ankit Jalote. Detection and prevention of stack buffer overflow attacks. *Commun. ACM*, 48(11):50–56, November 2005.
29. Carl E. Landwehr, Alan R. Bull, John P. McDermott, and William S. Choi. A taxonomy of computer program security flaws. *ACM Comput. Surv*., 26(3):211–254, September 1994.
30. Fangfei Liu, Yuval Yarom, Qian Ge, Gernot Heiser, and Ruby B. Lee. Last-level cache side-channel attacks are practical. In *Proceedings of the 2015 IEEE Symposium on Security and Privacy*, SP '15, pages 605–622, Washington, DC, USA, 2015. IEEE Computer Society.
31. Robert Martin, John Demme, and Simha Sethumadhavan. Timewarp: Rethinking timekeeping and performance monitoring mechanisms to mitigate side-channel attacks. In *Proceedings of the 39th Annual International Symposium on Computer Architecture*, ISCA '12, pages 118–129, Washington, DC, USA, 2012. IEEE Computer Society.

32. Y. Mo and B. Sinopoli. Secure control against replay attacks. In *2009 47th Annual Allerton Conference on Communication, Control, and Computing (Allerton*), pages 911–918, Sept 2009.
33. Guido Roßling and Marius Muller. Social engineering: A serious underestimated problem. In *Proceedings of the 14th Annual ACM SIGCSE Conference on Innovation and Technology in Computer Science Education*, ITiCSE ’09, pages 384–384, New York, NY, USA, 2009. ACM.
34. Julian L. Rrushi. *SCADA Protocol Vulnerabilities*, pages 150–176. Springer Berlin Heidelberg, Berlin, Heidelberg, 2012.
35. Hovav Shacham. The geometry of innocent flesh on the bone: Return-into-libc without function calls (on the x86). In *Proceedings of the 14th ACM Conference on Computer and Communications Security*, CCS ’07, pages 552–561, New York, NY, USA, 2007. ACM.
36. Yasser Shoukry, Paul Martin, Paulo Tabuada, and Mani Srivastava. *Non-invasive Spoofing Attacks for Anti-lock Braking Systems*, pages 55–72. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.
37. Andr´e Teixeira, Daniel P´erez, Henrik Sandberg, and Karl Henrik Johansson. Attack models and scenarios for networked control systems. In *Proceedings of the 1st International Conference on High Confidence Networked Systems*, HiCoNS ’12, pages 55–64, New York, NY, USA, 2012. ACM.
38. Tim Thornburgh. Social engineering: The ”dark art”. In *Proceedings of the 1st Annual Conference on Information Security Curriculum Development*, InfoSecCD ’04, pages 133–135, New York, NY, USA, 2004. ACM.
39. Yuval Yarom and Katrina Falkner. Flush+reload: A high resolution, low noise, L3 cache side-channel attack. In *Proceedings of the 23rd USENIX Conference on Security Symposium*, SEC’14, pages 719–732, Berkeley, CA, USA, 2014. USENIX Association.

Appendix A. Top 20 list from US News list of Top Engineering Schools and Three Military Universities and Academies

University	Public / Private	# of Students	Degrees Offered	Courses offered with security and trust in cyber-physical systems themes	Labs with security themes	Links	Summary
Georgia Institute of Technology Atlanta, GA	Public	Undergradute: 9418 Graduate: 3985	**Undergraduate** [BS] Computer Science [BS] Electrical Engineering [BS] Computer Engineering **Graduate** [MS] Cybersecurity [MS] Computer Science [MS] Computational Science and Engineering [MS] Electrical & Computer Engineering [PhD] Electrical and Computer Engineering [PhD] Computational Science and Engineering [PhD] Computer Science	**Undergraduate** [CS] 4235 Intro to Information Security [CS] 4237 Computer and Network Security [CS] 4432 Information Systems Design [ECE] 4112 Internetwork Security **Graduate** [CS] 7292 Reliability and Security in Computer Architecture [ECE] 8813 Intro to Cyber-Physical Systems Security	- CS department advertises cybersecurity research category and Architecture category; Systems Software & Security Lab very active - CS & Engineering department advertises cybersecurity research category - Have a group called 'Ubiquitous Computing Group' but doesn't deal with large systems, more day to day level activity	Courses: https://oscar.gatech.edu/pls/bprod/bwckctlg.p_disp_dyn_ctlg Research: http://www.scs.gatech.edu/content/groups-labs http://www.cse.gatech.edu/content/cybersecurity	✓Focused degree offered ✓Cybersecurity out of classroom focus ✓Some graduate level specific courses offered ✗Lack of specific undergraduate classes offered

Massachusetts Institute of Technology Cambridge, MA	Private	Undergraduate: 2479 Graduate: 3263	**Undergraduate** [BS] Electrical Science and Engineering (Course 6-1) [BS] Computer Science and Engineering (Course 6-3) [BS] Electrical Engineering and Computer Science (Course 6-2) **Graduate** [MS] Master's of Engineering (Course 6-P) [ME] Electrical Engineering and Computer Science [MS] Electrical Engineering and Computer Science [PhD] Computational Science and Engineering [PhD] Electrical Engineering and Computer Science	**Undergraduate** [Foundation] 6.033 Computer System Engineering **Graduate** [CS] 6.857 Network and Computer Security [CS] 6.858 Computer Systems Security [CS] 6.824 Distributed Computer Systems Engineering	- Cybersecurity@ CSAIL working toward solutions for the whole security spectrum - Host a Cybersecurity Professional Education six week long seminar for companies to enroll and learn about information and system security	Courses: http://eecsappsrv.mit.edu/students/ Research: http://web.mit.edu/research/ Professional Program: http://web.mit.edu/professional/digital-programs/online-course/cybersecurity/index.html CSAIL: http://cybersecurity.csail.mit.edu/	✓Cybersecurity out of classroom focus ✗ Major lack of specific courses offered at both undergraduate and graduate levels ✗ No specific degree offered

Stanford University Stanford, CA	Private	Undergraduate: 1526 Graduate: 3583	**Undergraduate** [BS] Computer Science [BS] Electrical Engineering **Graduate** [MS] Computer Science [MS] Electrical Engineering [Cert] Cyber Security	**Undergraduate** [CS] 203: Cybersecurity: A Legal and Technical Perspective [CS] 240: Advanced Topics in Operating Systems (PreReq: CS 140 Operating Systems and Programing) [CS] 155: Computer and Network Security [CS] 255: Introduction to Cryptography [CS] 55N: Freshman seminar: Great Ideas in Computer Security and Cryptography [CS] 255: Introduction to Cryptography and Computer Security [CS] 259: Security Analysis of Network Protocols [CS] 355: Topics in Cryptography [CS] 251: Cryptocurrencies, blockchains, and smart contracts [CS] 142: Web Programming and Security	- Computer Systems Laboratory is a joint lab of the Departments of Electrical Engineering and Computer Science, and within the Lab is the Stanford Robust Systems Group that deals exactly with these systems; another group in the Lab is the Ubiquitous Computing group - Stanford Secure Computer group deals with system security within the Computer Security Lab	Courses: https://explorecourses.stanford.edu/search Research: https://engineering.stanford.edu/research-and-faculty/institutes-labs-and-centers Stanford cybersecurity: https://cybersecurity.stanford.edu/ Secure Computing Systems: http://www.scs.stanford.edu/ Computer Security Lab: http://seclab.stanford.edu/	✓Specific certificate offered at graduate level ✓ Some thematic courses offered ✓Cybersecurity out of classroom focus

University of California-Berkeley Berkeley, CA	Public	Undergraduate: 3272 Graduate: 1946	**Undergraduate** [BS] Electrical Engineering and Computer Sciences **Graduate** [MS] Computer Science [PhD] Computer Science [MS] Electrical Engineering and Computer Sciences [ME] Electrical Engineering and Computer Sciences [PhD] Electrical Engineering and Computer Sciences [OM] Cybersecurity	**Graduate** [CS] 261 Security in Computer Systems [CS] 262B Advanced Topics in Computer Systems	- Team for Research in Ubiquitous Secure Technology (TRUST) is focused on the development of cyber security science and technology that will radically transform the ability of organizations to design, build, and operate trustworthy information systems for the nation's critical infrastructure (host a 9 week summer residency to 'prepare grads') - The Center for Long-Term Cybersecurity- information technology security - ASPIRE lab works on resilient systems, but no projects right now with large system resilience - CESR lab works on security but on	Courses: http://guide.berkeley.edu/courses/ Research: https://www2.eecs.berkeley.edu/Research/Areas/CS/ CLTC: https://cltc.berkeley.edu/about-us/ ASPIRE: https://aspire.eecs.berkeley.edu/projects/ CESR: https://evidencebasedsecurity.org/ FORCES: https://www.cps-forces.org/index.html ICSI:	✓Focused degree offered ✓Cybersecurity out of classroom focus ✗ Serious lack of thematically specific courses offered

					the internet and only has one project dealing with online markets - **FORCES** is designed to help protect the nation's critical infrastructure from attack and to ensure its robust, secure and efficient operation. - International Computer Science Institute (ICSI) is affiliated with the school and advertises Network Security as a research category but doesn't have any projects related underway	https://www.icsi.berkeley.edu/icsi/about	
California Institute of Technology Pasadena, CA	Private	Undergraduate: 473 Graduate: 543	**Undergraduate** [BS] Computer Science [BS] Electrical Engineering **Graduate** [MS] Computer Science [MS] Electrical Engineering [PhD] Computer Science [PhD] Electrical Engineering	none found	CTME hosts two day Cyber security seminar for businesses in July	Courses: http://www.catalog.caltech.edu/documents/79-catalog_16_17_part5.pdf	✗ No specific degree offered ✗ No thematically specific courses offered ✗ Minimal cybersecurity out of classroom focus

University of Illinois Champaign, IL	Public	Undergraduate: 9145 Graduate: 3422	**Undergraduate** [BS] Computer Engineering [BS] Electrical Engineering [BS] Computer Science **Graduate** [OM] Computer Security [MS] Computer Science [PhD] Computer Science [MS] Electrical and Computer Engineering [ME] Electrical and Computer Engineering [PhD] Electrical and Computer Engineering	**Undergraduate** [CS] 425 Distributed Systems (PreReq- Real Time Systems) [CS] 461 and 463 Computer Security I and II (PreReq- System Programming)	- Digital/Cyber Security and Nuclear Security research project currently underway - Illinois Cyber Security Scholars Program (ICSSP) is a two year program for law students and offers CyberCorps scholarship for those students	ECE courses: http://catalog.illinois.edu/undergraduate/engineer/departments/electrical-computer-engin/#courseinventory Computer Science courses: http://catalog.illinois.edu/undergraduate/engineer/departments/comp-sci/#courseinventory Research: http://engineering.illinois.edu/research/interdisciplinary-research-themes/i	✓Focused degree offered ✓Cybersecurity out of classroom focus ✗ Lack of thematically specific courses offered

						ndex.html Digital/Cyber Security research project: http://engineering.illinois.edu/research/strategic-research-initiatives/cyber-and-nuclear-security.html	
University of Michigan Ann Arbor, MI	Public	Undergraduate: 6556 Graduate: 3515	**Undergraduate** [BS] Computer Science [BS] Electrical Engineering [BS] Computer Engineering **Graduate** [MS] Electrical and Computer Engineering [ME] Electrical and Computer Engineering [PhD] Electrical and Computer Engineering [MS] Computer Science and Engineering [ME] Computer Science and Engineering [PhD] Computer Science and Engineering	**Undergraduate** - EECS 388. Introduction to Computer Security (PreReq: Data Structures and Algorithms) **Graduate** - EECS 588. Computer and Network Security (graduate) - EECS 475: Introduction to Cryptography - EECS 575: Advanced Cryptography - EECS 598: Medical Device Security	- Center for Computer Security and Society (C2S2) - RobustNet Research Group (more mobile based but still security based) - Security and Privacy Research Group (SPQR) - Center for Future Architectures Research collaborates with many schools to build scalable systems	Courses: http://www.engin.umich.edu/college/academics/bulletin/courses Computing research: http://arc.umich.edu/ RobustNet: http://vhosts.eecs.umich.edu/robustn	✓Cybersecurity out of classroom focus ✗ No focused degree offered ✗ Lack of thematically specific courses offered

						et//about.html	

Carnegie Mellon Pittsburgh, PA	Private	Undergraduate: 1780 Graduate: 1850	**Undergraduate** [BS] Electrical and Computer Engineering (offers Security track) [BS] Computer Science **Graduate** [MS] Electrical and Computer Engineering [PhD] Electrical and Computer Engineering [MS] Computer Science [PhD] Computer Science	**Undergraduate** [ECE]18-451 Networked Cyber Physical Systems [ECE]18-487 Introduction to Computer & Network Security & Applied Cryptography [ECE]18-632 Introduction to Hardware Security [ECE]18-651 Networked Cyber-Physical Systems [CS] 15-316 Software Foundations of Security and Privacy [CS]15-349 Introduction to Computer and Network Security (only offered in Qatar location) [CS]15-392 Special Topic: Secure Programming [CS]15-487 Introduction to Computer & Network Security & Applied Cryptography	Projects: Cyber-Security Threats to Industrial Control Systems; Trusted Computing; A Static Approach to Operating System Security IV; Continuous Authentication of Computer User: How to Avoid Computer Tailgating and Ensure Computer Security; Robust, Secure, Efficient Cyber-Physical Systems; Cross-Layer Self-Configuration for Secure and Resilient Networking - CyLab Security and Privacy Institute	Courses: http://coursecatalog.web.cmu.edu/carnegieinstituteoftechnology/departmentofelectricalandcomputerengineering/courses/ Program: http://www.ece.cmu.edu/news/story/2015/01/cyber-physical-systems.html CS Research: https://www.cylab.cmu.edu/research/projects/research-area/trustworthy-computing.html 1. https://www.cylab	✓Cybersecurity out of classroom focus ✓ Good amount of courses offered ✗ No thematic degree offered

						.cmu.edu/research/projects/2013/cybersecurity-threats-industrial-control-systems.html#sthash.Em9gXskd.dpuf 2. https://www.cylab.cmu.edu/research/projects/2009/trusted-computing.html 3. https://www.cylab.cmu.edu/research/projects/2012/static-operating-system-security.html 4. https://www.cylab.cmu.edu/research/projects/2010/continuous-	

						authentication.html#sthash.B5TtPWIv.dpuf 5. https://www.cylab.cmu.edu/research/projects/2012/robust-secure-efficient-systems.html 6. https://www.cylab.cmu.edu/research/projects/2013/cross-layer-self-configuration-networking.html#sthash.hRdcpmHl.dpuf 7. https://nsf.gov/awardsearch/showAward?AWD_ID=0955111&HistoricalAwards	

						=false CyLab: https://www.cylab.cmu.edu/about/index.html	

Cornell University Ithaca, NY	Private	Undergraduate: 3078 Graduate: 904	**Undergraduate** [BS] Computer Science **Graduate** [MS] Computer Science [ME] Computer Science [ME] Electrical and Computer Engineering [PhD] Electrical and Computer Engineering	**Professional Level/ Upper Division Undergrad** [CS] 5430 - System Security (PreReq: CS 4410 - Operating Systems) [CS] 5431 - Practicum in System Security (Corequisite: CS 5430) [CS] 5435 - Security and Privacy Concepts in the Wild (offered at NYC campus) (PreReqs: CS 2800 - Discrete Structures or CS 4820 - Introduction to Analysis of Algorithms) [CS] 5438 - Security and Privacy: Practice and Case Studies (offered at NYC campus) [CS] 5831 - Security Protocols and Privacy (PreReqs: CS 2800 - Discrete Structures and CS 4810 [Introduction to Theory of Computing]) [CS] 6113 - Language-Based Security (PreReqs: CS 4110 - Programming Languages and Logics or CS 6110 - Advanced Programming Languages) **Graduate** [CS] 7493 - Computer Security Seminar (PHD)	- Security Research section in CS department - Projects: Security modeling; Frenetic (network communication project to make network integration more intelligent and secure) - Advertise cybersecurity research grants and interested faculty on the Research homepage	ECE courses: https://classes.cornell.edu/browse/roster/FA17/subject/ECE CS courses: https://classes.cornell.edu/browse/roster/FA17/subject/CS Security research: https://www.cs.cornell.edu/research/security Frenetic: http://frenetic-lang.org/	✓ Some thematic courses offered ✓ Cybersecurity out of classroom focus ✗ No specific degrees offered

Purdue West Lafayette, IN	Public	Undergraduate: 8705 Graduate: 3463	**Undergraduate** [BS] Computer Science [BS] Electrical Engineering [BS] Computer Engineering **Graduate** [MS] Computer Science [PhD] Computer Science [MS] Computational Science and Engineering [PhD] Computational Science and Engineering [MS] Electrical Engineering [PhD] Electrical Engineering	**Undergraduate** [ECE] 40400 - Introduction to Computer Security (PreReq: ECE 36800 Data Structure) (Elective) [CS] 42600 - Computer Security (PreReq: CS 35400 Operating Systems) [CS] 30200 - Operating Systems [CS] 30600 - Computers In Society [CS] 37200 - Web Application Development [CS] 44500 - Computer Security **Graduate** [CS] 52800 - Network Security (PreReq: CS 52600 Information Security) (graduate) [CS] 52700 - Software Security (PreReq: CS 52600 Information Security) (graduate) [CS] 52600 - Information Security (PreReq: CS 50300 Operating Systems)	- Purdue Malware Lab - FBI Cyber Crime Task Force - High Performance Computing and Cyberinfrastructure Research Lab - Cybersecurity program advertises an IT focus	Courses: https://selfservice.mypurdue.purdue.edu/prod/bwckctlg.p_disp_dyn_ctlg? Research: https://engineering.purdue.edu/VPR/CORES/ptUnit?unit=Technology Lab: https://polytechnic.purdue.edu/facilities/high-performance-computing-and-cyberinfrastructure-research-lab IT Cybersecurity program: https://po	✓Cybersecurity out of classroom focus ✓ Some security classes at undergraduate and graduate level ✗ No specific degree offered

						lytechnic.purdue.edu/degrees/cybersecurity	
Princeton University Princeton, NJ	Private	Undergraduate: 670 Graduate: 619	**Undergraduate** [BS] Computer Science [BS] Electrical Engineering **Graduate** [MS] Computer Science [PhD] Computer Science [ME] Electrical Engineering [PhD] Electrical Engineering	**Undergraduate** [ELE] 386 Cyber Security (PreReq: COS 109 Computers in Our World)	- Involved in Frenetic project - More involved on the Policy end cyber-security wise	Courses: https://registrar.princeton.edu/course-offerings/	✗ No specific degree offered ✗ Serious lack of courses offered ✗ Minimal cybersecurity out of classroom focus

University of Texas - Austin Austin, TX	Public	Undergraduate: 7700 Graduate: 2149	**Undergraduate** [BS] Computer Science [BS] Electrical Engineering **Graduate** [ME] ECE - Software Engineering and Systems [PhD] ECE - Software Engineering and Systems [ME] ECE - Architecture, Computer Systems & Embedded Systems [PhD] ECE - Architecture, Computer Systems & Embedded Systems [MS] Computer Science [PhD] Computer Science	**Undergraduate** [CS] 361. Introduction to Computer Security. (PreReq: CS 429. Computer Organization and Architecture) (Elective) [CS] 361C. Information Assurance and Security. (PreReq: CS 429. Computer Organization and Architecture) [CS] 361S. Network Security and Privacy. (PreReq: CS 429. Computer Organization and Architecture) [CS] 356: Networks [CS] 361: Introduction to Computer Security [CS] 361S: Network Security and Privacy [CS] 371D: Distributed Computing [CS] 378: Ethical Hacking [CS] 380D: Distributed Computing I [CS] 395T: Cyber-physical systems [CS] 396M Advanced Networking Protocols	Networking Research Lab has one project with large system resilience	CS Courses: https://www.cs.utexas.edu/undergraduate-program/academics/curriculum/courses ; https://www.cs.utexas.edu/research/areas/security Network Research Lab: http://www.cs.utexas.edu/users/lam/NRL/	✓ Good amount of classes offered in cyber security ✗ No specific degree offered ✗ Minimal cybersecurity out of classroom focus
Northwestern University Evanston, IL	Private	Undergraduate: 1895 Graduate: 329	**Undergraduate** [BS] Computer Science [BS] Electrical Engineering [BS] Computer Engineering **Graduate** [MS] Computer Science [PhD] Computer Science [MS] Electrical Engineering [PhD] Electrical Engineering [MS] Computer Engineering [PhD] Computer Engineering	**Undergraduate** [EECS] 350: Introduction To Computer Security (PreReq: Intro to Computer Systems) (not currently on available course roster) [EECS] 354: Network Penetration And Security (PreReq: Intro to Computer Systems) (not currently on available course roster)	- Project: Hardware/Compiler Co-Design Approaches to Software Protection - Many cyber security topics in Law school, less in CS; cyber security program more focused on IT	Courses: http://www.mccormick.northwestern.edu/eecs/courses/ Research: http://cucis.ece.northwestern.edu/projects/	✓Some security courses offered ✗ Minimal cybersecurity out of classroom focus ✗ No specific degree offered

Johns Hopkins Baltimore, MD	Private	N/A	**Undergraduate** [BS] Computer Science [BS] Electrical Engineering [BS] Computer Engineering **Graduate** [MS] Cybersecurity/ Security Informatics [MS] Electrical and Computer Engineering [PhD] Electrical and Computer Engineering [MS] Computer Science [PhD] Computer Science	**Undergraduate** [CS] EN.600.424. Network Security. (PreReqs: EN.600.226 Data Structures and (EN.600.344 Computer Network Fundamentals or EN.600.444 Computer Networks)) [CS] EN.600.443. Security & Privacy in Computing. **Graduate** [CS] EN.600.643. Advanced Topics in Computer Security [CS] EN.600.668. Advanced Topics in Software Security [ISI] EN.650.624. Advanced Network Security. (PreReq: EN.600.424. Network Security)	none found (only have Information Security groups)	Courses: https://sis.jhu.edu/classes/ Info Security Research: https://www.cs.jhu.edu/research/information-security/	✓Specific degree offered ✓ Some specific courses offered ✗ No cybersecurity out of classroom focus
University of Wisconsin Madison, WI	Public	Undergraduate: 5000 Graduate: 1600	**Undergraduate** [BS] Computer Engineering [BS] Electrical Engineering [BS] Computer Sciences **Graduate** [MS] Computer Science [PhD] Computer Science [MS] Electrical Engineering [PhD] Electrical Engineering	none found	host a Lockdown 2017 Cybersecurity conference in July	Courses: https://portal.sispub.wisc.edu:7052/psp/public/EMPLOYEE/HRMS/c/COMMUNITY_ACCESS.CLASS_SEARCH.GBL Conference: https://lockdown.it.wisc.edu/logistics-2/	✗ No specific degree offered ✗ No specific courses offered ✗ Minimal cybersecurity out of classroom focus

Texas A&M College Station, TX	Public	Undergraduate: 12646 Graduate: 3621	**Undergraduate** [BS] Computer Engineering (EE or CS Track) [BS] Computer Science [BS] Electrical Engineering [Minor] Cybersecurity **Graduate** [MS] Computer Engineering (EE or CS Track) [ME] Computer Engineering (EE or CS Track) [PhD] Computer Engineering (EE or CS Track) [MS] Computer Science [PhD] Computer Science [MS] Electrical Engineering [ME] Electrical Engineering [PHD] Electrical Engineering	**Undergraduate** [CSCE] 465 Computer and Network Security (PreReqs: CSCE 313 Intro to Computer Systems and CSCE 315 Programming Studio) [CSCE] 489 SPTP: Software Security (PreReq: CSCE 315 Programming Studio) **Graduate** [CSCE] 665 ADV Network & Security	Have a 'Cybersecurity Center' where one research theme is Resilient Adversary-Tolerant Systems	Courses: https://compass-ssb.tamu.edu/pls/PROD/bwckschd.p_disp_dyn_sched Research: https://cybersecurity.tamu.edu/research/	✓ Minor offered on theme ✓ Cybersecurity out of classroom focus ✗ Lack of specific courses offered
Virginia Tech Blacksburg, VA	Public	Undergraduate: 7906 Graduate: 2083	**Undergraduate** [BS] Computer Engineering [BS] Computer Science [BS] Electrical Engineering [Cert] Cybersecurity **Graduate** [MS] Computer Engineering [ME] Computer Engineering [PhD] Computer Engineering [MS] Computer Science and Applications [PhD] Computer Science and Applications [MS] Electrical Engineering [ME] Electrical Engineering [PhD] Electrical Engineering [Cert] Cybersecurity	**Undergraduate** [CS] 4264 Principles of Computer Security (PreReq: CS 3214: Introduction to computer systems) [ECE] 4560 Computer and Network Security Fundamentals (PreReq: ECE 4564- Network Application Design) [ECE] 4944 Cybersecurity Seminar (PreReq: CS 2504 Intro Computer Organization)	- ARIAS Research Lab: Secure Programming Skills Assessment Exam Development and Curriculum Revision (this project) - Center for Embedded Systems for Critical Applications (CESCA) lab doesn't have any projects related now but is a good infrastructure for a related	Courses: http://www.cs.vt.edu/undergraduate/courses Cyber research: http://www.cnsr.ictas.vt.edu/	✓ Cybersecurity out of classroom focus ✓ Security degree offered at undergraduate and graduate level ✗ Lack of specific courses in CPS

					project to come about - Security and Privacy in Cyber-physical Systems project: e-healthcare systems and smart grid - Hume Center is currently constructing a lab focused in CPS Security - Cyber-Physical System Security advertised in Hume Center		
Columbia New York City, NY	Private	Undergraduate: 1583 Graduate: 3101	**Undergraduate** [BS] Computer Science [BS] Computer Science and Engineering [BS] Electrical Engineering [BS] Electrical Engineering and Computer Science **Graduate** [MS] Computer Science [MS] Computer Science and Engineering [MS] Electrical Engineering [MS] Electrical Engineering and Computer Science	**Undergraduate** [CS] W4180 Network Security [EE] E4905 Topics In EE & CE: Cybersecurity **Graduate** [CS] W4180 Network Security [CS] W4187 Security Architecture and Engineering [CS] E6185 Intrusion Detection [CS] E6183 Security [CS] E6185 Intrusion and Anomaly Detection Systems	- Data Science Institute addresses cybersecurity; has a lab section researching computer architecture and hardware security but no relevant projects found - Cryptography lab in Data Science Institute - Public policy related seminars on cybersecurity hosted on campus and	Courses: http://www.columbia.edu/cu/bulletin/uwb/ CASTL: http://castl.cs.columbia.edu/	✓ Masters core track offered in cyber security ✓ Some courses offered ✓ Cybersecurity out of classroom focus ✗ No specific degree offered

					programs within the liberal arts school		
Duke University Durham, NC	Private	Undergraduate: 663 Graduate: 988	**Undergraduate** [BSE] Electrical and Computer Engineering [BS] Computer Science **Graduate** [MS] Computer Science [PhD] Computer Science [MS] Electrical and Computer Engineering [PhD] Electrical and Computer Engineering	**Undergraduate** [ECE] 356 Computer Network Architecture. (PreReq: CPS 310: Operating Systems)	more focused on law school, not in CS program	Courses: http://soc.siss.duke.edu/psp/CSSOC01/EMPLOYEE/HRMS/c/COMMUNITY_ACCESS.SSS_BROWSE_CATLG.GBL?PORTALPARAM_PTCNAV=HC_SSS_BROWSE_CATLG_GBL4&EOPP.SCNode=HRMS&EOPP.S	✗ No specific degree offered ✗ No specific courses offered ✗ No cybersecurity out of classroom focus

						CPortal=EMPLOYEE&EOPP.SCName=DU_PUBLIC_SCHEDULECATALOG_VIE&EOPP.SCLabel=&EOPP.SCPTcname=DU_SC_SP_PUBLIC_SCHEDULECATAL&FolderPath=PORTAL_ROOT_OBJECT.PORTAL_BASE_DATA.CO_NAVIGATION_COLLECTIONS.DU_PUBLIC_SCHEDULECATALOG_VIE.DU_S200901121425362238532670&IsFolder=false	

						Law Cybersecurity Conference: https://law.duke.edu/video/lens-conference-2017-cyber-security-surveillance-future-cybersecurity/	

Penn State University Park, PA	Public	Undergraduate: 7846 Graduate: 1421	**Undergraduate** [BS] Computer Engineering [BS] Computer Science [BS] Electrical and Computer Engineering Technology [BS] Electrical Engineering [BS] Electrical Engineering Technology **Graduate** [OM] Master of Professional Studies in Information Sciences - Cybersecurity and Information Assurance [MS] Computer Science and Engineering [ME] Computer Science and Engineering [PhD] Computer Science and Engineering [MS] Electrical Engineering [PhD] Electrical Engineering	**Undergraduate** [CS] 438 Computer Network Architecture and Programming (PreReqs: CMPSC 221 Object Oriented Programming with Web-Based Applications, CMPSC 312 Computer Organization and Architecture) [CS] 443 Introduction to Computer and Network Security (PreReq: CMPSC 473 Operating Systems Design & Construction) [IST] 451: Network Security	- Cyber Security Lab: Security of Cyber-Physical Systems (CPS); NSF: CPS-security: attack-resilient automated control of UAVs - College of Information Sciences and Technology	Courses: http://bulletins.psu.edu/bulletins/bluebook/university_course_descriptions.cfm Research: https://s2.ist.psu.edu/ Cyber Security Lab: https://s2.ist.psu.edu/	✓ Specific degree offered ✓ Cybersecurity out of classroom focus ✗ Lack of specific courses offered
United States Military Academy-West Point West Pint, NY	Public	(Near 100 in Computer Science)	**Undergraduate Majors** Computer Science Electrical Engineering	none found	- Cyber Research Center (CRC)	Courses: http://www.usma.edu/crc/SitePages/Education.aspx CRC: http://www.usma.edu/crc/SitePages/About.aspx	

United States Naval Academy Annapolis, MD	Public	N/A	**Undergraduate Majors** Electrical Engineering Computer Engineering Cyber Operations Computer Science	[ECE] 310 Applications of Cyber Engineering [ECE] 312 Applications of Cyber Engineering for Systems Engineering [ECE] 356 Computer Networks with Security Applications [CS] 430 Computer and Network Security [CS] 432 Advanced Computer and Network Security [Cyber Science] 110 Cyber Security 1 [Cyber Science] 202 Cyber Systems Engineering (cyber-physical system course) [Cyber Science] 304 Social Engineering, Hacktivism, and Information Operations in the Cyber Domain [Cyber Science] 308 Security Fundamental Principles	- Center for Cyber Security Studies - Computer, Network, and Usable Security faculty research area	CCSS: https://www.usna.edu/CyberCenter/ Courses: https://www.usna.edu/Academics/Majors-and-Courses/Course-Catalog.php	

Naval Postgraduate School Monterey, CA	Public	Undergraduate: N/A Graduate: 1039	[Cert] Cyber Warfare [Cert] Wireless Network Security [Cert] Cyber Systems [Cert] Cyber Warfare [Cert] Cyber Security Fundamentals [Cert] Cyber Security Defense [Cert]Cyber Security Adversarial Techniques Certificate [MS] Applied Cyber Operations [MS] Cyber Systems and Operations [MS] Computer Science [MS] Identity Management and Cyber Security [PhD] Computer Science	[ECE] 2700 Introduction to Cyber Systems [ECE] 3730 Cyber Network and Physical Infrastructures [ECE] 4715 Cyber System Vulnerabilities and Risk Assessment [ECE] 4735 Telecommunications Systems Security [ECE] 4770 Wireless Communication Network Security [ECE] 4765 Cyber Warfare [CS] 3600 Introduction to Computer Security [CS] 3645 Cyber Threats and Mitigation [CS] 3670 Secure Management of Systems [CS] 3690 Network Security [CS] 4600 Secure System Principles [CS] 4650 Fundamentals of Information Systems Security Engineering [CS] 4679 Advances in Cyber Security Operations [CS] 4684 Cyber Security Incident Response and Recovery [CS] 4690 Security for Cyber-Physical Systems	- Introductory Computer Security Laboratory - Computer Information Security Lab - SCIF Security Lab - CS department researches network & mobile wireless security, information security & assurance, and cyber systems and operations - Cyber Battle Lab - Highly Trustworthy Systems Lab - Center for Cyber Warfare	Catalog: http://web.nps.edu/Academics/GeneralCatalog/index.htm	

Appendix B. Curriculum for DIA Education Program on Cyber Attack Resilience for Cyber Physical Systems

The ongoing UVA developed 2 course DIA education program is referred to as Cyber Resiliency for DoD Acquisition Programs. Each of the two courses is comprised of 10 classes, each of two-hour duration. The specific material for each class is based upon the results of an ongoing DoD/OSD sponsored Systems Engineering research program led by UVA through the Stevens Institute led multi-university, OSD sponsored UARC. Each class had an individually selected lecturer, chosen based upon the relationship between their individual research activities and the desired content of the lecture. To assure continuity from lecture to lecture and between lectures and laboratory activities, Professor Horowitz, the Principal Investigator for the OSD- sponsored research program, organized the course content, selected the lecturers and participated in all of the classes. While UVA faculty members were the major providers of individual lectures (15 of the 20 classes), Virginia Commonwealth University provided 4 lectures, and one class lecturer was a current employee of a commercial company hired in an adjunct role. Note that the logistics associated with managing the multi-lecturer program caused the order of lectures to deviate from the plan (2 cases), but the 2-lecture overview that started DIA 101 served to create resilience to the change in the order of lectures regarding the students' ability to absorb the material. The 40 hour program includes 10 hours of laboratory-focused classes. These classes provided teams of 3 students each with the opportunity to conduct hands-on efforts involving a hardware/software mock-up of a military weapon system and the SecurITree attack tree tool. In addition to the time spent in the UVA-provided laboratory space, the students were provided with the necessary hardware and support software to conduct laboratory-related efforts at home. The design of the mock-up was a derivative of a research-supporting mock-up that was developed by UVA as part of the OSD/SERC sponsored research activity referred to above. The cost to UVA of hardware for the UVA laboratory and for student home use (on loan to them) was $2000. The 18 licenses for the SecurITree tool use were provided at no cost by AMANZA, the company that offers this tool on the open market.

Education Curriculum Plan
Cyber Resiliency for DoD Acquisition Programs 101/102

DIA 101

Class 1 - The underlying concepts for applying resilience-based solutions to cyber security defense (2 hours) - Horowitz
Class 2 – System-Aware Cybersecurity (2 hours)- Horowitz
Classes 3,4 & 5 – Technology Prototypes (4 hours)
- UAV and Automobile/ MSI Product Description and Demo (2 hours) – Jones
- 3D Printing (2 hours) – Garner
- Sensor-focused Cyber Attacks and Solution Opportunities (2 hours) – Bezzo

Class 6 – Fault Tolerant Systems Design Principles (2 hours) – Williams
Class 7 - Attack Trees (2 hours)– Elks
Class 8– Attack Taxonomy- Davidson
Class 9 – Cybersecurity-related Human Factors Issues (2 hours) – Kim, Horowitz
Class 10 – Term Project Plan - Hands-on Laboratory Exercise (2 hours)-Horowitz

DIA 102

Class 1 - Hands-on attack laboratory activity (2 hours) – Huband
Class 2 – Hands-on Decision support tool laboratory activity
Classes 3, 4,5, 6 , 7 – Security Solution Selection (10 hours)

Analysis - Beling, Fleming
Attack Tree Analysis - Elks
SysML – Fleming, Bakirtzis
Machine Learning - Adams

Classes 8, 9 – Presentations of Individual Team Exercise Results and Class Evaluation of Results (4 hours) - Horowitz
Class 10 – Summary and Discussion – Horowitz

Appendix C – Laboratory Use Case

Building upon a laboratory use case that supports the ongoing UVA-led cyber attack resiliency research effort sponsored by DoD, the selected use case for the DIA education program is a hypothetical land mine weapon system.

- Purpose: Prevent, when and where necessary, via the use of a rapidly deployable land mine system, adversaries from trespassing into geographic areas that are close to strategically sensitive locations.
- Prohibited Area : 5-10 acres of open field space
- Land Mines: About 50 short range mines distributed over the prohibited area
- Operation: Operator remote-control of individual or groups of mines, based upon surveillance of the prohibited area (operator located 250-500 feet away from prohibited area).
- Prohibited Area Surveillance: The operator has binoculars to support visual observation and also is supported by real-time video information provided by a separately operated UAV.
- Land-mine design features: The land mines are designed so that they provide regular situation awareness reports (seconds apart). This includes reports on their location (GPS-based), their on-off status, their acceptance of commands, their actual firings, etc. Furthermore, their SW can only be modified by electrically disconnecting their computer from the land mine, and removal results in destroying that computer. Designed this way to avoid debugging related SW errors (now providing collateral value related to possible cyber attacks).
- Requirements for Avoiding Errors: Significant concerns about detonating land mines in cases where non-adversarial people, by chance, enter the prohibited area, and also about failing to detonate land mines when an adversary is approaching the strategically-sensitive location via the prohibited area.
- Operator Functions: The operator can cause individual or designated groups of land mines to detonate through the weapon system's integrated communication network, designed to permit needed communications between the land mine system operator, the individual land mines, the command center that the operator reports to, the UAV video collection subsystem, and the UAV pilot.
- Operator Control Station: Hand held computer provides operator observation of weapon status, weapon control inputs, video observation, and supports required digital situation awareness-related reporting to the command center and the UAV pilot.
- Command Center Controls: The command center digitally provides weapon control information for the operator (determines weapon system on/off periods, designates periods of higher likelihood of attack, provides forecasts of possible approach direction to the prohibited area, enables operation with/without UAV support, etc). As determined by either the operator or the command center, out of norm situations can be supported through rapid message communications between command center and the operator.
- Forensics: All subsystems collect and store forensic information for required post-mission analysis purposes
- Rapid Deployment Support: All subsystems enable rapid deployment support features, including automated confirmation testing of the integrated system.
- UAV Video Collection/Distribution Subsystem: Piccolo

The hardware/software mock-up description is contained in a file hosted by the SERC UARC and available through their web site, along with this report.